NCI BASELINE SECURITY ASSESSMENT

Prepared For: Sample Report

Prepared By: Jason Dahl
NETWORK CENTER, INC.

PURPOSE

Security Assessments are a critical part of creating a secure Information Technology environment and identifying and managing risks that a customer currently faces. The NCI Vulnerability Assessment focuses on locating and reporting vulnerabilities affecting the confidentiality, integrity, and availability of information systems. Vulnerabilities discovered fall in to two categories:

- Remote - an attacker would need access to the local network to exploit
- Local- an attacker would need access to the local host or require interaction from the user to exploit

These vulnerabilities can be exploited by spyware applications, hackers, worms, and viruses. Conducting a vulnerability assessment aids in building a strong information security program by reducing the overall risk of known threats and weaknesses. The goal of this assessment is to assist [customer] [in making sure your overall cyber security program and infrastructure is secure from attackers and ensure the customer is compliant with government requirements specific to the industry. In this report, we will identify critical weaknesses, unpatched systems, hidden vulnerabilities, loopholes, and potential gaps in your cyber security program.

THE ASSESSMENT & TEAM

This vulnerability assessment was performed for [customer] [using an industry leading network analysis tool at the request of the customer. Any equipment connected to the network at the time of assessment, such as desktops, servers, and networking systems, were analyzed. Systems that were not powered on or were disconnected from the network at the time of the assessment could not be assessed. The scanning device relies on network connections to discover, connect to, and scan remote machines. Findings from the Assessment will detail IPs scanned, systems discovered, and identified critical and high severity vulnerabilities.

Network Center, Inc. (NCI) is well versed in cybersecurity consulting and auditing. The Network Security Team holds several industry recognized certifications such as CompTIA Security+, Certified Information Systems Security Professional (CISSP), Certified Cloud Security Professional (CCSP), and several application security specific certifications. Jason Dahl, Sr. Security Engineer at NCI oversaw this assessment. Dahl has 23+ years of technical and cyber security experience within the Department of Defense and private sector. He's held positions both within leadership and senior technical level Security+.

METHODOLOGY

NCI adheres to the following Vulnerability Assessment methodology to ensure the accuracy and thoroughness of the reporting.

Information Gathering

NCI begins by getting a better understanding of the client environment such as hosts, networks, and devices it desires to have accessed. This information should include a Network Diagram, IT Asset Inventory, and list of hosts and subnets to be evaluated. In addition, information from Active Directory is looked at and permissions and attack paths tested.

Testing

NCI performs a Network Vulnerability Assessment to detect all active systems on the client network and determine which services each system is using and analyzes each for vulnerabilities. Active systems on the network are detected by sending a variety of requests to each host or network identified in the information gathering phase of the assessment. If the device receives a response from any of the requests, it will be added to a list of active hosts. Because systems running host-based firewalls may not respond to these requests, NCI asks that the client disable all host-based firewall applications running on internal network hosts prior to the Vulnerability Assessment.

Reporting

When the assessment is complete, NCI reviews the results reported by the scanning system. The results are analyzed and compiled based on criticality and provided to the client. Vulnerabilities discovered are rated by the Common Vulnerability Scoring System (CVSS). The findings from each system that had one or more critical vulnerability ratings are reported by the service where the vulnerability was discovered. Recommendations are provided within the report but are not requirements and the implementation of any of the recommendations is at the discretion of the client.

Understanding CVSS

The Common Vulnerability Scoring System (CVSS) is a widely used vulnerability rating framework that provides a uniform rating system across all software and hardware platforms. A base CVSS Score is calculated from the Impact and Exploitability of the vulnerability. To determine the overall impact of a vulnerability, the Impact is calculated from the Confidentiality Impact, Integrity Impact, and Availability Impact. The Exploitability of the vulnerability is calculated from the AccessVector, AccessComplexity, and Authentication. For complete details on the CVSS, please reference the following website: https://www.first.org/cvss/user-guide

CVSS Ratings

Low	Medium	High	Critical
0.1 - 3.9	4.0 – 6.9	7.0 – 8.91	9.0 – 10

EXECUTIVE ANALYSIS & FINDINGS

The Vulnerability Assessment process identified **47 critical** and **117 high priority** vulnerabilities on various [customer] systems. Out of those 47 critical vulnerabilities, 11 were found to be unique. The criticality of each system should be evaluated, and most critical systems addressed first. System criticality should be determined by the type of information stored and processed by the system, the type of job function the system supports, and the complexity of the operating system. Machines should also be prioritized by the level of risk associated with the number of vulnerabilities discovered.

Below is the suggested order in which [customer] [should address the recommendations contained in this report:

1. Remediate all critical and high vulnerabilities, including upgrading EOL products
2. Strengthen password policy, unless implementing MFA within next few months
3. Separation of duties for Administrator tasks
4. Deploy Microsoft SYSMON
5. Implement Microsoft BitLocker
6. Apply CIS Operating System Hardening Benchmarks, Level 1, BL, and NG

The table on page 5 lists all systems discovered during the assessment. Each system is identified by the IP address, system name (if available), operating system (if available) and number of vulnerabilities found. Systems containing one or more vulnerabilities are reported with a bar chart that identifies the two most critical categories.

Systems running Windows operating systems are also shown whether the scanning device had the ability to perform administrative registry checks. Allowing administrative registry checks enhances the level of vulnerability discovery, as well as reduces the number of false positives reported and the risk of adversely affecting systems being assessed.

Conclusions:
[customer] understands the importance of protecting the confidentiality, integrity, and availability of the information contained within its systems. Continued monitoring of controls and systems will be crucial to maintaining [customer] [’s IT security. Findings and recommendations have been discussed with [customer] [management. If there are any questions concerning this assessment, report, or recommended action items, please feel free to contact Network Center, Inc. This documentation is considered confidential and is property of Network Center, Inc. The unauthorized copying or distribution of this document is strictly prohibited.

Name	IP	Operating System	Critical	High
Desktop-1	192.168.0.1	Microsoft Windows 10 Pro	5	2
DESKTOP-2	192.168.0.1	Microsoft Windows Server 2019 Standard	4	1
DESKTOP-3	192.168.0.1	Microsoft Windows 10 Pro	3	9
DESKTOP-4	192.168.0.1	Linux Kernel 3.1	2	0
DESKTOP-5	192.168.0.1	Microsoft Windows 10 Pro	2	5
DESKTOP-6	192.168.0.1	Microsoft Windows 10 Pro	2	8
DESKTOP-7	192.168.0.1	Microsoft Windows 10 Pro	2	7
DESKTOP-8	192.168.0.1	Microsoft Windows 10 Pro	2	5
DESKTOP-9	192.168.0.1	Microsoft Windows 10 Pro	2	6
DESKTOP-10	192.168.0.1	Microsoft Windows 10 Pro	2	3
DESKTOP-11	192.168.0.1	Microsoft Windows 10 Pro	2	3
DESKTOP-12	192.168.0.1	Microsoft Windows Server 2019 Standard	2	0
DESKTOP-13	192.168.0.1	Microsoft Windows 10 Pro	2	2
DESKTOP-14	192.168.0.1	EthernetBoard OkiLAN 8100e	1	1
DESKTOP-15	192.168.0.1	Microsoft Windows 10 Pro	1	1
DESKTOP-16	192.168.0.1	Microsoft Windows 10 Pro	1	12
DESKTOP-17	192.168.0.1	Microsoft Windows 10 Pro	1	4
DESKTOP-18	192.168.0.1	Microsoft Windows 10 Pro	1	4
DESKTOP-19	192.168.0.1	Microsoft Windows 10 Pro	1	5
DESKTOP-20	192.168.0.1	Microsoft Windows 10 Pro	1	5
DESKTOP-21	192.168.0.1	Microsoft Windows 10 Pro	1	6
DESKTOP-22	192.168.0.1	Microsoft Windows 10 Pro	1	5
DESKTOP-23	192.168.0.1	Microsoft Windows 10 Pro	1	5
DESKTOP-24	192.168.0.1	Microsoft Windows 10 Pro	1	6
DESKTOP-25	192.168.0.1	Microsoft Windows 10 Pro	1	2
DESKTOP-26	192.168.0.1	Microsoft Windows 10 Pro	1	1
DESKTOP-27	192.168.0.1	SonicWALL	0	0
DESKTOP-28	192.168.0.1	NEC SIP Device	0	0
DESKTOP-29	192.168.0.1	Roku 3810X	0	0
DESKTOP-30	192.168.0.1	Linux Kernel 4.9	0	0
DESKTOP-40	192.168.0.1	Linux Kernel 2.6	0	0
DESKTOP-41	192.168.0.1		0	0
DESKTOP-42	192.168.0.1	Microsoft Windows 10	0	0
DESKTOP-43	192.168.0.1	Microsoft Windows 10	0	0
DESKTOP-44	192.168.0.1	Microsoft Windows 10	0	0
DESKTOP-45	192.168.0.1	Microsoft Windows 10	0	0
DESKTOP-46	192.168.0.1	Microsoft Windows 10	0	0
DESKTOP-47	192.168.0.1	Microsoft Windows 10	0	0
DESKTOP-48	192.168.0.1	Microsoft Windows 10 Pro	0	0
DESKTOP-49	192.168.0.1	Microsoft Windows 10	0	0
DESKTOP-50	192.168.0.1	Samsung Electronics UN65NU710D 1.0	0	0
DESKTOP-51	192.168.0.1		0	0
DESKTOP-52	192.168.0.1		0	0

CRITICAL VULNERABILITIES

Vulnerability	KB5012647: Windows 10 version 1809 Security Update (April 2022)					
Synopsis	The remote Windows host is affected by multiple vulnerabilities.					
Severity	Critical					
CVSS Score	10			Exploitable		
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	MainServer2	MAINSERVER2	
	192.168.0.1	445	cifs	Mainserver3	MAINSERVER3	

Description

The remote Windows host is missing security update 5012591. It is, therefore, affected by multiple vulnerabilities:

- An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges. (CVE-2022-26790, CVE-2022-26828, CVE-2022-26827, CVE-2022-26807, CVE-2022-26796, CVE-2022-26798, CVE-2022-26808, CVE-2022-26810, CVE-2022-26803, CVE-2022-26802, CVE-2022-26801, CVE-2022-26794, CVE-2022-26792, CVE-2022-26904, CVE-2022-26788, CVE-2022-26793, CVE-2022-26914, CVE-2022-26789, CVE-2022-26797, CVE-2022-26787, CVE-2022-24549, CVE-2022-26795, CVE-2022-26786, CVE-2022-24496, CVE-2022-24544, CVE-2022-24540, CVE-2022-24489, CVE-2022-24486, CVE-2022-24481, CVE-2022-24479, CVE-2022-24527, CVE-2022-24474, CVE-2022-24521, CVE-2022-24550, CVE-2022-24499, CVE-2022-24547, CVE-2022-24546, CVE-2022-24494, CVE-2022-24542, CVE-2022-24530)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-26831, CVE-2022-26915, CVE-2022-24538, CVE-2022-24484, CVE-2022-26784)

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-26824, CVE-2022-26812, CVE-2022-26919, CVE-2022-26918, CVE-2022-26809, CVE-2022-26825, CVE-2022-26916, CVE-2022-26819, CVE-2022-26817, CVE-2022-26815, CVE-2022-26814, CVE-2022-26823, CVE-2022-26811, CVE-2022-26829, CVE-2022-26821, CVE-2022-26917, CVE-2022-26820, CVE-2022-26826, CVE-2022-26818, CVE-2022-26822, CVE-2022-26813, CVE-2022-24545, CVE-2022-24541, CVE-2022-24492, CVE-2022-24491, CVE-2022-24537, CVE-2022-24536, CVE-2022-24487, CVE-2022-24534, CVE-2022-24485, CVE-2022-24533, CVE-2022-26903, CVE-2022-24495, CVE-2022-24528, CVE-2022-21983, CVE-2022-22008, CVE-2022-24500)

- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-26920, CVE-2022-26816, CVE-2022-24493, CVE-2022-24539, CVE-2022-24490, CVE-2022-26783, CVE-2022-26785, CVE-2022-24498, CVE-2022-24483)

Solution

Apply Cumulative Update 5012647

Additional Resources

https://support.microsoft.com/en-us/help/5012647

Vulnerability	Microsoft SQL Server Unsupported Version Detection					
Synopsis	An unsupported version of a database server is running on the remote host.					
Severity	Critical					
CVSS Score	10			Exploitable		
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Mainserver	MAINSERVER	

Description

According to its self-reported version number, the installation of Microsoft SQL Server on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of Microsoft SQL Server that is currently supported.

Additional Resources

http://www.nessus.org/u?d4418a57

Comments

N/A

Vulnerability	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities					
Synopsis	The SSH service running on the remote host is affected by multiple vulnerabilities.					
Severity	Critical					
CVSS Score	10			Exploitable	false	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	22	ssh			

Description

According to its self-reported version in its banner, Dropbear SSH running on the remote host is prior to 2016.74. It is, therefore, affected by the following vulnerabilities:

- A format string flaw exists due to improper handling of string format specifiers (e.g., %s and %x) in usernames and host arguments. An unauthenticated, remote attacker can exploit this to execute arbitrary code with root privileges. (CVE-2016-7406)
- A flaw exists in dropbearconvert due to improper handling of specially crafted OpenSSH key files. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-7407)
- A flaw exists in dbclient when handling the -m or -c arguments in scripts. An unauthenticated, remote attacker can exploit this, via a specially crafted script, to execute arbitrary code. (CVE-2016-7408)
- A flaw exists in dbclient or dropbear server if they are compiled with the DEBUG_TRACE option and then run using the -v switch. A local attacker can exploit this to disclose process memory. (CVE-2016-7409)

Solution

Upgrade to Dropbear SSH version 2016.74 or later.

Additional Resources

https://matt.ucc.asn.au/dropbear/CHANGES

Comments

N/A

Vulnerability	KB5012599: Windows 10 Version 2004 / 20H2 / n 21H1 Security Update (April 2022)					
Synopsis	The remote Windows host is affected by multiple vulnerabilities.					
Severity	Critical					
CVSS Score	10			Exploitable		
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	
	192.168.0.1	445	cifs	Desktop1	Desktop1	

Description

The remote Windows host is missing security update 5012591. It is, therefore, affected by multiple vulnerabilities:

- An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges. (CVE-2022-26789, CVE-2022-26786, CVE-2022-26802, CVE-2022-26803, CVE-2022-26801, CVE-2022-26796, CVE-2022-26787, CVE-2022-26797, CVE-2022-26827, CVE-2022-26810, CVE-2022-26808, CVE-2022-26798, CVE-2022-24549, CVE-2022-26795, CVE-2022-26791, CVE-2022-26794, CVE-2022-26904, CVE-2022-26792, CVE-2022-26807, CVE-2022-26788, CVE-2022-26828, CVE-2022-26790, CVE-2022-26914, CVE-2022-26793, CVE-2022-24496, CVE-2022-24544, CVE-2022-24540, CVE-2022-24489, CVE-2022-24488, CVE-2022-24486, CVE-2022-24481, CVE-2022-24479, CVE-2022-24527, CVE-2022-24474, CVE-2022-24521, CVE-2022-24550, CVE-2022-24499, CVE-2022-24547, CVE-2022-24546, CVE-2022-24494, CVE-2022-24542, CVE-2022-24530)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-26831, CVE-2022-26915, CVE-2022-24538, CVE-2022-24484, CVE-2022-26784)

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-26917, CVE-2022-26916, CVE-2022-26812, CVE-2022-26811, CVE-2022-26919, CVE-2022-26823, CVE-2022-26809, CVE-2022-26824, CVE-2022-26818, CVE-2022-26815, CVE-2022-26814, CVE-2022-26822, CVE-2022-26918, CVE-2022-26829, CVE-2022-26820, CVE-2022-26826, CVE-2022-26819,

CVE-2022-26825, CVE-2022-26817, CVE-2022-26821, CVE-2022-26813, CVE-2022-24545, CVE-2022-24541, CVE-2022-24492, CVE-2022-24491, CVE-2022-24537, CVE-2022-24536, CVE-2022-24487, CVE-2022-24534, CVE-2022-24485, CVE-2022-24533, CVE-2022-26903, CVE-2022-24495, CVE-2022-24528, CVE-2022-23257, CVE-2022-21983, CVE-2022-22009, CVE-2022-22008, CVE-2022-24500) - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-26816, CVE-2022-26920, CVE-2022-24493, CVE-2022-24539, CVE-2022-24490, CVE-2022-26783, CVE-2022-26785, CVE-2022-24498, CVE-2022-24483)
Solution
Apply Security Update 5012599
Additional Resources
https://support.microsoft.com/en-us/help/5012591
Comments
N/A

Vulnerability	Compromised Windows System (hosts File Check)					
Synopsis	The remote Windows host may be compromised.					
Severity	Critical					
CVSS Score	10			**Exploitable**		
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	192.168.0.1	445	cifs	Desktop25	DESKTOP25	
	192.168.0.1	445	cifs	Desktop45	DESKTOP45	
Description						
The remote Windows host uses the file 'System32\drivers\etc\hosts' to fix the name resolution of some sites to localhost or internal systems. Some viruses or spyware modify this file to prevent antivirus software or other security software from obtaining updates. Nessus has found one or more suspicious entries in this file that may prove the remote host is infected by a malicious program.						
Solution						
Remove the suspicious entries from the host file, update your antivirus software, and remove any malicious software.						
Additional Resources						
http://www.nessus.org/u?b5c6c90d						
Comments						
N/A						

Vulnerability	Apple QuickTime Unsupported on Windows					
Synopsis	Apple QuickTime is installed on the remote Windows host.					
Severity	Critical					
CVSS Score	10			**Exploitable**		
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	192.168.0.1	445	cifs	Desktop25	DESKTOP25	
	192.168.0.1	445	cifs	Desktop5	DESKTOP5	
Description						
Apple no longer supports any version of QuickTime on Windows. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is						

likely to contain security vulnerabilities.
Note that the last version of QuickTime released for Windows had known vulnerabilities related to processing atom indexes. A remote attacker can exploit these, by convincing a user to view a malicious website or open a crafted file, to cause heap corruption within QuickTime, resulting in the execution of arbitrary code in the context of the user or process running QuickTime.

Solution

Uninstall Apple QuickTime.

Additional Resources

https://support.apple.com/en-us/HT205771
https://www.zerodayinitiative.com/advisories/ZDI-16-242/
https://www.zerodayinitiative.com/advisories/ZDI-16-241/
https://www.us-cert.gov/ncas/alerts/TA16-105A

Comments

N/A

Vulnerability	KB5009543: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (January 2022)					
Synopsis	The remote Windows host is affected by multiple vulnerabilities.					
Severity	Critical					
CVSS Score	10			Exploitable	true	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop23	DESKTOP23	
	192.168.0.1	445	cifs	Desktop17	DESKTOP17	
	192.168.0.1	445	cifs	Desktop31	DESKTOP31	
	192.168.0.1	445	cifs	Desktop30	DESKTOP30	

Description

The remote Windows host is missing security update 5009543.
It is, therefore, affected by multiple vulnerabilities:
- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-21849, CVE-2022-21850, CVE-2022-21851, CVE-2022-21874, CVE-2022-21878, CVE-2022-21892, CVE-2022-21893, CVE-2022-21922, CVE-2022-21928, CVE-2022-21958, CVE-2022-21959, CVE-2022-21960, CVE-2022-21961, CVE-2022-21962, CVE-2022-21963)
- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-21876, CVE-2022-21880, CVE-2022-21904, CVE-2022-21915)
- A security feature bypass vulnerability exists. An attacker can exploit this and bypass the security feature and perform unauthorized actions compromising the integrity of the system/application. (CVE-2022-21894, CVE-2022-21900, CVE-2022-21905, CVE-2022-21913, CVE-2022-21924, CVE-2022-21925)
- A session spoofing vulnerability exists. An attacker can exploit this to perform actions with the privileges of another user. (CVE-2022-21836)
- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-21843, CVE-2022-21848, CVE-2022-21883, CVE-2022-21889, CVE-2022-21890)
- An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges. (CVE-2022-21833, CVE-2022-21834, CVE-2022-21835, CVE-2022-21838, CVE-2022-21857, CVE-2022-21859, CVE-2022-21860, CVE-2022-21862, CVE-2022-21863, CVE-2022-21864, CVE-2022-21866, CVE-2022-21867, CVE-2022-21868, CVE-2022-21870, CVE-2022-21871, CVE-2022-21873, CVE-2022-21875, CVE-2022-21879, CVE-2022-21881, CVE-2022-21884, CVE-2022-21885, CVE-2022-21895, CVE-2022-21897, CVE-2022-21901, CVE-2022-21902, CVE-2022-21903, CVE-2022-21908, CVE-2022-21910, CVE-2022-21914, CVE-2022-21916, CVE-2022-21919, CVE-2022-21920)

Solution

Apply Cumulative Update KB5009543.
Additional Resources
https://support.microsoft.com/en-us/help/5009543
Comments
N/A

Vulnerability	Adobe Reader <= 2015.006.30510 / 2017.011.30158 / 2020.006.20034 Multiple Vulnerabilities (APSB20-13)					
Synopsis	The version of Adobe Reader installed on the remote Windows host is affected by multiple vulnerabilities.					
Severity	Critical					
CVSS Score	10			**Exploitable**	true	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	192.168.0.1	445	cifs	Desktop5	Desktop5	
Description						
The version of Adobe Reader installed on the remote Windows host is a version prior or equal to 2015.006.30510, 2017.011.30158, or 2020.006.20034. It is, therefore, affected by multiple vulnerabilities. - Out-of-bounds read potentially leading to Information Disclosure (CVE-2020-3804, CVE-2020-3806) - Out-of-bounds write potentially leading to Arbitrary Code Execution (CVE-2020-3795) - Stack-based buffer overflow potentially leading to Arbitrary Code Execution (CVE-2020-3799) - Use-after-free potentially leading to Arbitrary Code Execution (CVE-2020-3792, CVE-2020-3793, CVE-2020-3801, CVE-2020-3802, CVE-2020-3805) - Memory address leak potentially leading to Information Disclosure (CVE-2020-3800) - Buffer overflow potentially leading to Arbitrary Code Execution (CVE-2020-3807) - Memory corruption potentially leading to Arbitrary Code Execution (CVE-2020-3797) - Insecure library loading (DLL hijacking) potentially leading to Privilege Escalation (CVE-2020-3803) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.						
Solution						
Upgrade to Adobe Reader version 2015.006.30518 or 2017.011.30166 or 2020.006.20042 or later.						
Additional Resources						
https://helpx.adobe.com/security/products/acrobat/apsb20-13.html						
Comments						
N/A						

Vulnerability	Apache Log4j Unsupported Version Detection					
Synopsis	A logging library running on the remote host is no longer supported.					
Severity	Critical					
CVSS Score	10			**Exploitable**		
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	192.168.0.1	445	cifs	Desktop22	DESKTOP22	
Description						
According to its self-reported version number, the installation of Apache Log4j on the remote host is no longer supported. Log4j reached its end of life prior to 2016. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.						
Solution						

Upgrade to a version of Apache Log4j that is currently supported. Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.
Additional Resources
http://www.nessus.org/u?59f655a2
Comments
N/A

Vulnerability	Apache Log4j 1.x Multiple Vulnerabilities					
Synopsis	A logging library running on the remote host has multiple vulnerabilities.					
Severity	Critical					
CVSS Score	10			**Exploitable**		
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	192.168.0.1	445	cifs	Desktop22	DESKTOP22	

Description
According to its self-reported version number, the installation of Apache Log4j on the remote host is 1.x and is no longer supported. Log4j reached its end of life prior to 2016. Additionally, Log4j 1.x is affected by multiple vulnerabilities, including: - Log4j includes a SocketServer that accepts serialized log events and deserializes them without verifying whether the objects are allowed or not. This can provide an attack vector that can be exploited. (CVE-2019-17571) - Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender. (CVE-2020-9488) - JMSSink uses JNDI in an unprotected manner allowing any application using the JMSSink to be vulnerable if it is configured to reference an untrusted site or if the site referenced can be accesseed by the attacker. (CVE-2022-23302) Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
Solution
Upgrade to a version of Apache Log4j that is currently supported. Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.
Additional Resources
https://logging.apache.org/log4j/1.2/
Comments
N/A

Vulnerability	Microsoft Office 365 Unsupported Channel Version Detection					
Synopsis	The remote host contains an unsupported Channel version of Microsoft Office 365.					
Severity	Critical					
CVSS Score	10			Exploitable		
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop39	DESKTOP39	
	192.168.0.1	445	cifs	Desktop34	DESKTOP34	
	192.168.0.1	445	cifs	Desktop37	DESKTOP37	

Description

According to its Channel version, the installation of Microsoft Office 365 on the remote Windows host is no longer supported. Refer to links in See Also for details on currently supported versions for each Channel.
- Current Channel: Updated once a month, on the second Tuesday of the month. Any given version of Current Channel is supported only until the next version of Current Channel is released, which is usually every month.
- Monthly Enterprise Channel: Any given version of Monthly Enterprise Channel is supported for two months. At any given time, there are always two versions of Monthly Enterprise Channel that are supported.
- Semi-Annual Enterprise Channel (Preview): Released with new features twice a year, on the second Tuesday in March and September (four months before those same new features are released in Semi-Annual Enterprise Channel).
- Semi-Annual Enterprise Channel: Any given version of Semi-Annual Enterprise Channel is supported for fourteen months. This means that the new version of Semi-Annual Enterprise Channel that is released in January is supported until March of the following year, and the July release is supported until September of the following year. At any given time, there are always two supported versions, except during the first two months of the year, when there will be 3 supported versions.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a Channel version of Microsoft Office 365 that is currently supported.

Additional Resources

http://www.nessus.org/u?b09fa171
http://www.nessus.org/u?cebfe0cb

Comments

N/A

Vulnerability	SSL Version 2 and 3 Protocol Detection					
Synopsis	The remote service encrypts traffic using a protocol with known weaknesses.					
Severity	Critical					
CVSS Score	10			Exploitable		
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	1433	mssql	MainServer2	MAINSERVER2	
	192.168.0.1	1433	mssql	Mainserver3	MAINSERVER3	
	192.168.0.1	443	www			

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:
- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.
An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between

the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.
Solution
Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.
Additional Resources
https://www.schneier.com/academic/paperfiles/paper-ssl.pdf http://www.nessus.org/u?b06c7e95 http://www.nessus.org/u?247c4540 https://www.openssl.org/~bodo/ssl-poodle.pdf http://www.nessus.org/u?5d15ba70 https://www.imperialviolet.org/2014/10/14/poodle.html https://tools.ietf.org/html/rfc7507 https://tools.ietf.org/html/rfc7568
Comments
N/A

Vulnerability	SNMP Agent Default Community Names					
Synopsis	The community names of the remote SNMP server can be guessed.					
Severity	Critical					
CVSS Score	10			**Exploitable**	false	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	192.168.0.1	161	snmp			

Description
It is possible to obtain the default community names of the remote SNMP server. An attacker can use this information to gain more knowledge about the remote host or to change the configuration of the remote system (if the default community allows such modifications).
Solution
Disable the SNMP service on the remote host if you do not use it, filter incoming UDP packets going to this port, or change the default community string.
Additional Resources
Comments
N/A

HIGH VULNERABILITIES

Vulnerability	Apple iCloud 7.x < 7.15 Multiple Vulnerabilities					
Synopsis	An iCloud software installed on the remote Windows host is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	9.3			Exploitable	true	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop19	DESKTOP19	

Description

According to its version, the iCloud application installed on the remote Windows host is 7.x prior to 7.15. It is, therefore, affected by multiple vulnerabilities:

- Multiple arbitrary code execution vulnerabilities exist with in the WebKit due to multiple memory corruption issues. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2019-8783, CVE-2019-8784, CVE-2019-8811, CVE-2019-8814, CVE-2019-8815, CVE-2019-8816, CVE-2019-8819, CVE-2019-8820, CVE-2019-8821, CVE-2019-8822, CVE-2019-8823)

Solution

Upgrade to iCloud version 7.15 or later.

Additional Resources

https://support.apple.com/HT210728

Comments

N/A

Vulnerability	Apple iCloud 7.x < 7.18 Multiple Vulnerabilities					
Synopsis	An iCloud software installed on the remote Windows host is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	9.3			Exploitable	true	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop19	DESKTOP19	

Description

According to its version, the iCloud application installed on the remote Windows host is 7.x prior to 7.18. It is, therefore, affected by multiple vulnerabilities:

- A logic issue was addressed with improved restrictions. A file URL may be incorrectly processed. (CVE-2020-3885)

- A logic issue was addressed with improved restrictions. A download's origin may be incorrectly associated. (CVE-2020-3887)
- A race condition was addressed with additional validation. An application may be able to read restricted memory. (CVE-2020-3894)

- An arbitrary code execution vulnerability exists within the WebKit due to maliciously crafted content issues. An unauthenticated, remote attacker can exploit this by processing maliciously crafted web content may lead to arbitrary code execution. (CVE-2020-3895, CVE-2020-3899, CVE-2020-3900)

- An arbitrary code execution vulnerability exists within the WebKit due to type confusion issues. A remote attacker may be able to cause arbitrary code execution. (CVE-2020-3897, CVE-2020-3901)

- An arbitrary code execution vulnerability exists within the WebKit due to input validation issues. An unauthenticated, remote attacker can exploit this by processing maliciously crafted web content may lead to arbitrary code execution. (CVE-2020-3902)

- An arbitrary code execution vulnerability exists within the WebKit due to buffer overflow issues. Multiple issues in libxml2. (CVE-2020-3909, CVE-2020-3910, CVE-2020-3911)

- An arbitrary code execution vulnerability exists within the WebKit due to use after free issues. An unauthenticated, remote attacker can exploit this by processing maliciously crafted web content may lead to arbitrary code execution. (CVE-2020-9783)

Solution

Upgrade to iCloud version 7.18 or later.

Additional Resources

https://support.apple.com/en-us/HT211107

Comments

N/A

Vulnerability	Adobe Reader < 17.012.30227 / 17.012.30229 / 20.005.30331 / 20.005.30331 / 20.005.30334 / 20.005.30334 / 22.001.20112 / 22.001.20117 Multiple Vulnerabilities (APSB22-16)					
Synopsis	The version of Adobe Reader installed on the remote Windows host is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	9.3			**Exploitable**	false	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	192.168.0.1	445	cifs	Desktop19	DESKTOP19	
	192.168.0.1	445	cifs	Desktop29	DESKTOP29	
	192.168.0.1	445	cifs	Desktop32	DESKTOP32	
	192.168.0.1	445	cifs	Desktop25	DESKTOP25	
	192.168.0.1	445	cifs	Desktop23	DESKTOP23	
	192.168.0.1	445	cifs	Desktop17	DESKTOP17	
	192.168.0.1	445	cifs	Desktop5	DESKTOP5	
	192.168.0.1	445	cifs	Desktop31	DESKTOP31	
	192.168.0.1	445	cifs	Desktop22	DESKTOP22	
	192.168.0.1	445	cifs	Desktop21	DESKTOP21	
	192.168.0.1	445	cifs	Desktop39	DESKTOP39	
	192.168.0.1	445	cifs	Desktop33	DESKTOP33	
	192.168.0.1	445	cifs	Desktop34	DESKTOP34	
	192.168.0.1	445	cifs	Desktop24	DESKTOP24	
	192.168.0.1	445	cifs	Desktop27	DESKTOP27	
	192.168.0.1	445	cifs	Desktop30	DESKTOP30	
	192.168.0.1	445	cifs	Desktop41	DESKTOP41	
	192.168.0.1	445	cifs	Desktop45	DESKTOP45	
	192.168.0.1	445	cifs	Desktop37	DESKTOP37	

Description

The version of Adobe Reader installed on the remote Windows host is a version prior to 17.012.30227, 17.012.30229, 20.005.30331, 20.005.30331, 20.005.30334, 20.005.30334, 22.001.20112, or 22.001.20117. It is, therefore, affected by multiple vulnerabilities.

- Acrobat Reader DC ActiveX Control versions 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must visit an attacker-controlled web page. (CVE-2021-44702)

- Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. (CVE-2021-44706, CVE-2021-45064)

- Acrobat Reader DC ActiveX Control versions 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file or visit an attacker-controlled web page. (CVE-2021-44739)

- Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Access of Memory Location After End of Buffer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
(CVE-2021-45067)

- Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file. (CVE-2022-24091, CVE-2022-24092)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Adobe Reader version 17.012.30227 / 17.012.30229 / 20.005.30331 / 20.005.30331 / 20.005.30334 / 20.005.30334 / 22.001.20112 / 22.001.20117 or later.

Additional Resources

https://cwe.mitre.org/data/definitions/121.html
https://cwe.mitre.org/data/definitions/122.html
https://cwe.mitre.org/data/definitions/125.html
https://cwe.mitre.org/data/definitions/353.html
https://cwe.mitre.org/data/definitions/416.html
https://cwe.mitre.org/data/definitions/657.html
https://cwe.mitre.org/data/definitions/787.html
https://cwe.mitre.org/data/definitions/824.html
https://helpx.adobe.com/security/products/acrobat/apsb22-16.html

Comments

N/A

Vulnerability	KB5010342: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (February 2022)					
Synopsis	The remote Windows host is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	9.3			Exploitable	true	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop19	DESKTOP19	
	192.168.0.1	445	cifs	Desktop29	DESKTOP29	
	192.168.0.1	445	cifs	Desktop38	DESKTOP38	
	192.168.0.1	445	cifs	Desktop20	DESKTOP20	
	192.168.0.1	445	cifs	Desktop25	DESKTOP25	
	192.168.0.1	445	cifs	Desktop23	DESKTOP23	
	192.168.0.1	445	cifs	Desktop17	DESKTOP17	
	192.168.0.1	445	cifs	Desktop31	DESKTOP31	
	192.168.0.1	445	cifs	Desktop27	DESKTOP27	
	192.168.0.1	445	cifs	Desktop30	DESKTOP30	
	192.168.0.1	445	cifs	Desktop37	DESKTOP37	

Description

The remote Windows host is missing security update 5010342. It is, therefore, affected by multiple vulnerabilities

- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-21993, CVE-2022-21998)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-22002)

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-21992, CVE-2022-21995)

- An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges. (CVE-2022-21989, CVE-2022-21994, CVE-2022-21997, CVE-2022-21999, CVE-2022-22000, CVE-2022-22001)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Apply Security Update 5010342

Additional Resources

https://support.microsoft.com/en-us/help/5010342

Comments

N/A

Vulnerability	Adobe Acrobat < 17.012.30227 / 17.012.30229 / 20.005.30331 / 20.005.30331 / 20.005.30334 / 20.005.30334 / 22.001.20112 / 22.001.20117 Multiple Vulnerabilities (APSB22-16)					
Synopsis	The version of Adobe Acrobat installed on the remote Windows host is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	9.3			**Exploitable**	false	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	192.168.0.1	445	cifs	Desktop38	DESKTOP38	

Description

The version of Adobe Acrobat installed on the remote Windows host is a version prior to 17.012.30227, 17.012.30229, 20.005.30331, 20.005.30331, 20.005.30334, 20.005.30334, 22.001.20112, or 22.001.20117. It is, therefore, affected by multiple vulnerabilities.

- Acrobat Reader DC ActiveX Control versions 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must visit an attacker-controlled web page. (CVE-2021-44702)

- Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. (CVE-2021-44706, CVE-2021-45064)

- Acrobat Reader DC ActiveX Control versions 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file or visit an attacker-controlled web page. (CVE-2021-44739)

- Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Access of Memory Location After End of Buffer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
(CVE-2021-45067)

- Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file. (CVE-2022-24091, CVE-2022-24092)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Adobe Acrobat version 17.012.30227 / 17.012.30229 / 20.005.30331 / 20.005.30331 / 20.005.30334 / 20.005.30334 / 22.001.20112 / 22.001.20117 or later.

Additional Resources

https://cwe.mitre.org/data/definitions/121.html
https://cwe.mitre.org/data/definitions/122.html
https://cwe.mitre.org/data/definitions/125.html

https://cwe.mitre.org/data/definitions/353.html https://cwe.mitre.org/data/definitions/416.html https://cwe.mitre.org/data/definitions/657.html https://cwe.mitre.org/data/definitions/787.html https://cwe.mitre.org/data/definitions/824.html https://helpx.adobe.com/security/products/acrobat/apsb22-16.html
Comments
N/A

Vulnerability	QuickTime < 7.7.6 Multiple Vulnerabilities (Windows)					
Synopsis	The remote Windows host contains an application that is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	9.3			**Exploitable**	false	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	192.168.0.1	445	cifs	Desktop25	DESKTOP25	

Description

The version of Apple QuickTime installed on the remote Windows host is prior to 7.7.6. It is, therefore, affected by the following vulnerabilities

- A memory corruption flaw exists when handling specially crafted RLE encoded videos due to user-supplied input not being properly sanitized. (CVE-2014-1391)
- A buffer overflow flaw exists when parsing specially crafted MIDI files due to user-supplied input not being properly validated. (CVE-2014-4350)
- A buffer overflow flaw exists when parsing specially crafted M4A files due to user-supplied input not being properly validated. (CVE-2014-4351)
- A memory corruption flaw exists in the mvhd atom when handling malformed version numbers and flags due to not properly sanitizing user-supplied input. (CVE-2014-4979)

Successful exploitation of these issues by a remote attacker can result in program termination or arbitrary code execution, subject to the user's privileges.

Solution

Upgrade to QuickTime 7.7.6 or later.

Additional Resources

https://support.apple.com/en-us/HT203092
https://www.securityfocus.com/archive/1/533790/30/0/threaded

Comments

N/A

Vulnerability	QuickTime < 7.7.5 Multiple Vulnerabilities (Windows)					
Synopsis	The remote Windows host contains an application that may be affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	9.3			Exploitable	false	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop25	DESKTOP25	

Description

The version of QuickTime installed on the remote Windows host is earlier than 7.7.5. It is, therefore, reportedly affected by the following vulnerabilities:

- Out-of-bounds byte swapping issues exist in the handling of QuickTime image descriptions and 'ttfo' elements. (CVE-2013-1032, CVE-2014-1250)

- An uninitialized pointer issue exists in the handling of track lists. (CVE-2014-1243)

- Buffer overflow vulnerabilities exist in the handling of H.264 encoded movie files, 'ftab' atoms, 'ldat' atoms, PSD images, and 'clef' atoms. (CVE-2014-1244, CVE-2014-1248, CVE-2014-1249, CVE-2014-1251)

- A signedness issue exists in the handling of 'stsz' atoms. (CVE-2014-1245)

- A memory corruption issue exists in the handling of 'dref' atoms. (CVE-2014-1247)

Successful exploitation of these issues could result in program termination or arbitrary code execution, subject to the user's privileges.

Solution

Upgrade to QuickTime 7.7.5 or later.

Additional Resources resources

https://www.zerodayinitiative.com/advisories/ZDI-14-044/
https://www.zerodayinitiative.com/advisories/ZDI-14-045/
https://www.zerodayinitiative.com/advisories/ZDI-14-046/
https://www.zerodayinitiative.com/advisories/ZDI-14-047/
https://www.zerodayinitiative.com/advisories/ZDI-14-048/
https://www.zerodayinitiative.com/advisories/ZDI-14-049/
https://support.apple.com/en-us/HT204527
https://lists.apple.com/archives/security-announce/2014/Feb/msg00002.html
https://www.securityfocus.com/archive/1/531268/30/0/threaded

Comments

N/A

Vulnerability	Adobe Reader < 17.011.30207 / 20.004.30020 / 21.011.20039 Multiple Vulnerabilities (APSB22-01)					
Synopsis	The version of Adobe Reader installed on the remote Windows host is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	9.3			Exploitable	false	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop23	DESKTOP23	
	192.168.0.1	445	cifs	Desktop31	DESKTOP31	
	192.168.0.1	445	cifs	Desktop30	DESKTOP30	

Description

The version of Adobe Reader installed on the remote Windows host is a version prior to 17.011.30207, 20.004.30020, or 21.011.20039. It is, therefore, affected by multiple vulnerabilities.

- Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. (CVE-2021-44701, CVE-2021-44704, CVE-2021-44705, CVE-2021-44706, CVE-2021-44710, CVE-2021-45062, CVE-2021-45064)

- Acrobat Reader DC ActiveX Control versions 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must visit an attacker controlled web page. (CVE-2021-44702)

- Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a stack buffer overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. (CVE-2021-44703)

- Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. (CVE-2021-44707, CVE-2021-45061, CVE-2021-45068)

- Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a heap overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. (CVE-2021-44708, CVE-2021-44709)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Adobe Reader version 17.011.30207 / 20.004.30020 / 21.011.20039 or later.

Additional Resources

https://cwe.mitre.org/data/definitions/20.html
https://cwe.mitre.org/data/definitions/121.html
https://cwe.mitre.org/data/definitions/122.html
https://cwe.mitre.org/data/definitions/125.html

https://cwe.mitre.org/data/definitions/190.html
https://cwe.mitre.org/data/definitions/284.html
https://cwe.mitre.org/data/definitions/416.html
https://cwe.mitre.org/data/definitions/476.html
https://cwe.mitre.org/data/definitions/657.html
https://cwe.mitre.org/data/definitions/787.html
https://cwe.mitre.org/data/definitions/788.html
https://cwe.mitre.org/data/definitions/824.html
https://helpx.adobe.com/security/products/acrobat/apsb22-01.html

Comments

N/A

Vulnerability	KB5011487: Windows 10 Version 20H2 / 21H1 / 21H2 Security Update (March 2022)					
Synopsis	The remote Windows host is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	9			Exploitable		
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop19	DESKTOP19	
	192.168.0.1	445	cifs	Desktop29	DESKTOP29	
	192.168.0.1	445	cifs	Desktop32	DESKTOP32	
	192.168.0.1	445	cifs	Desktop16	DESKTOP16	
	192.168.0.1	445	cifs	Desktop38	DESKTOP38	
	192.168.0.1	445	cifs	Desktop20	DESKTOP20	
	192.168.0.1	445	cifs	Desktop25	DESKTOP25	
	192.168.0.1	445	cifs	Desktop23	DESKTOP23	
	192.168.0.1	445	cifs	Desktop17	DESKTOP17	
	192.168.0.1	445	cifs	Desktop31	DESKTOP31	
	192.168.0.1	445	cifs	Desktop21	DESKTOP21	
	192.168.0.1	445	cifs	Desktop33	DESKTOP33	
	192.168.0.1	445	cifs	Desktop34	DESKTOP34	
	192.168.0.1	445	cifs	Desktop27	DESKTOP27	
	192.168.0.1	445	cifs	Desktop30	DESKTOP30	
	192.168.0.1	445	cifs	Desktop45	DESKTOP45	
	192.168.0.1	445	cifs	Desktop37	DESKTOP37	

Description

The remote Windows host is missing security update 5011487. It is, therefore, affected by multiple vulnerabilities:

- An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges. (CVE-2022-23283, CVE-2022-23284, CVE-2022-23291, CVE-2022-24459, CVE-2022-23296, CVE-2022-24507, CVE-2022-24454, CVE-2022-23298, CVE-2022-23290, CVE-2022-23288, CVE-2022-24525, CVE-2022-24460, CVE-2022-23299, CVE-2022-23293, CVE-2022-23287, CVE-2022-21967, CVE-2022-24505, CVE-2022-23286)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-21975, CVE-2022-23253)

- A security feature bypass vulnerability exists. An attacker can exploit this and bypass the security feature and perform unauthorized actions compromising the integrity of the system/application. (CVE-2022-24502)

- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2022-21977, CVE-2022-22010, CVE-2022-23281, CVE-2022-23297, CVE-2022-24503)

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2022-21990, CVE-2022-23285, CVE-2022-23294, CVE-2022-24508)

Solution

Apply Cumulative Update 5011487.

Additional Resources

Comments

N/A

Vulnerability	Zoom Client < 5.8.4 Multiple Vulnerabilities					
Synopsis	The remote host has an application installed that is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	7.5			Exploitable	true	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop19	DESKTOP19	
	192.168.0.1	445	cifs	Desktop29	DESKTOP29	
	192.168.0.1	445	cifs	Desktop32	DESKTOP32	
	192.168.0.1	445	cifs	Desktop25	DESKTOP25	
	192.168.0.1	445	cifs	Desktop23	DESKTOP23	
	192.168.0.1	445	cifs	Desktop31	DESKTOP31	
	192.168.0.1	445	cifs	Desktop21	DESKTOP21	
	192.168.0.1	445	cifs	Desktop33	DESKTOP33	
	192.168.0.1	445	cifs	Desktop24	DESKTOP24	
	192.168.0.1	445	cifs	Desktop30	DESKTOP30	
	192.168.0.1	445	cifs	Desktop37	DESKTOP37	

Description

The version of the Zoom Client installed on the remote host is prior to 5.8.4. It is, therefore, affected by the following vulnerabilities:

- An unspecified buffer overflow condition. An unauthenticated, remote attacker can exploit this to cause a denial-of-service condition or the execution of arbitrary code. (CVE-2021-34423)

- An unspecified information disclosure vulnerability. An unauthenticated, remote attacker can exploit this to disclose potentially sensitive information. (CVE-2021-34424)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Zoom Client for Meetings 5.8.4 or later.

Additional Resources

https://explore.zoom.us/en/trust/security/security-bulletin
https://support.zoom.us/hc/en-us/articles/201361953
https://support.zoom.us/hc/en-us/articles/201361963

Comments

N/A

Vulnerability	Apple iCloud < 7.12 Multiple Vulnerabilities					
Synopsis	An iCloud softare installed on the remote Windows host is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	7.5			Exploitable	true	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop19	DESKTOP19	
	192.168.0.1	445	cifs	Desktop5	DESKTOP5	

Description

According to its version, the iCloud application installed on the remote Windows host is prior to 7.12. It is, therefore, affected by multiple vulnerabilities:

- An arbitrary code execution vulnerability exists in SQLite & WebKit due to maliciously crafted content. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2019-8600, CVE-2019-6237, CVE-2019-8571, CVE-2019-8583, CVE-2019-8584, CVE-2019-8586, CVE-2019-8587, CVE-2019-8594, CVE-2019-8595, CVE-2019-8596, CVE-2019-8597, CVE-2019-8601, CVE-2019-8608, CVE-2019-8609, CVE-2019-8610, CVE-2019-8611, CVE-2019-8615, CVE-2019-8619, CVE-2019-8622, CVE-2019-8623, CVE-2019-8628)

- An privilege escalation vulnerability exists in SQLite due to an input validation and memory corruption issue. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2019-8577, CVE-2019-8602)

- An arbitrary memory read vulnerability exists in SQLite due to improper input validation. An unauthenticated, remote attacker can exploit this to read restricted memory. (CVE-2019-8598)

Solution

Upgrade to iCloud version 7.12 or later.

Additional Resources

https://support.apple.com/en-us/HT210125

Comments

N/A

Vulnerability	VLC < 3.0.9 Multiple Vulnerabilities					
Synopsis	The remote Windows host contains a media player that is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	7.5			Exploitable		
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop32	DESKTOP32	
	192.168.0.1	445	cifs	Desktop38	DESKTOP38	
	192.168.0.1	445	cifs	Desktop39	DESKTOP39	
	192.168.0.1	445	cifs	Desktop34	DESKTOP34	
	192.168.0.1	445	cifs	Desktop37	DESKTOP37	

Description

The version of VLC media player installed on the remote Windows host is prior to 3.0.9. It is, therefore, affected by multiple vulnerabilities:

- An exploitable denial-of-service vulnerability exists in the resource record-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing compressed labels in mDNS messages, the compression pointer is followed without

checking for recursion, leading to a denial of service. An attacker can send an mDNS message to trigger this vulnerability (CVE-2020-6071).

- An exploitable code execution vulnerability exists in the label-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing compressed labels in mDNS messages, the rr_decode function's return value is not checked, leading to a double free that could be exploited to execute arbitrary code. An attacker can send an mDNS message to trigger this vulnerability (CVE-2020-6072).

- An exploitable denial-of-service vulnerability exists in the TXT record-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing the RDATA section in a TXT record in mDNS messages, multiple integer overflows can be triggered, leading to a denial of service. An attacker can send an mDNS message to trigger this vulnerability (CVE-2020-6073).

- An exploitable denial-of-service vulnerability exists in the message-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing mDNS messages, the implementation does not keep track of the available data in the message, possibly leading to an out-of-bounds read that would result in a denial of service. An attacker can send an mDNS message to trigger this vulnerability (CVE-2020-6077).

- An exploitable denial-of-service vulnerability exists in the message-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing mDNS messages in mdns recv, the return value of the mdns_read_header function is not checked, leading to an uninitialized variable usage that eventually results in a null pointer dereference, leading to service crash. An attacker can send a series of mDNS messages to trigger this vulnerability (CVE-2020-6078).

- An exploitable denial-of-service vulnerability exists in the resource allocation handling of Videolabs libmicrodns 0.1.0. When encountering errors while parsing mDNS messages, some allocated data is not freed, possibly leading to a denial-of-service condition via resource exhaustion. An attacker can send one mDNS message repeatedly to trigger this vulnerability through decoding of the domain name performed by rr_decoder (CVE-2020-6079).

Solution

Upgrade to VLC version 3.0.9 or later.

Additional Resources

https://www.videolan.org/security/sb-vlc309.html

Comments

N/A

Vulnerability	Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU)					
Synopsis	The remote host is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	7.5			Exploitable		
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop32	DESKTOP32	
	192.168.0.1	445	cifs	Desktop38	DESKTOP38	
	192.168.0.1	445	cifs	Desktop34	DESKTOP34	
	192.168.0.1	445	cifs	Desktop30	DESKTOP30	

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 321, 8 Update 311, 11 Update 13, or 17 Update 1. It is, therefore, affected by multiple vulnerabilities as referenced in the October 2021 CPU advisory:

- Vulnerability in the Java SE product of Oracle Java SE (component: JavaFX (libxml)). The supported version that is affected is Java SE: 8u301. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE as well as unauthorized update, insert or delete access to some of Java SE accessible data and unauthorized read access to a subset of Java SE accessible data. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). (CVE-2021-3517)

- Vulnerability in the Java SE product of Oracle Java SE (component: Deployment). The supported version that is affected is Java SE: 8u301. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). (CVE-2021-35560)

- Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2021-35567)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Apply the appropriate patch according to the October 2021 Oracle Critical Patch Update advisory.

Additional Resources

https://www.oracle.com/a/tech/docs/cpuoct2021cvrf.xml
https://www.oracle.com/security-alerts/cpuoct2021.html#AppendixJAVA

Comments

N/A

Vulnerability	Apple QuickTime < 7.7.8 Multiple Arbitrary Code Vulnerabilities (Windows)					
Synopsis	The remote Windows host contains an application that is affected by multiple arbitrary code execution vulnerabilities.					
Severity	High					
CVSS Score	7.5			Exploitable	false	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop25	DESKTOP25	

Description

The version of Apple QuickTime installed on the remote Windows host is prior to 7.7.8. It is, therefore, affected by multiple arbitrary code execution vulnerabilities:
- A memory corruption issue exists due to improper validation of user-supplied input when handling URL atom sizes.

A remote attacker can exploit this issue by convincing a user to open a specially crafted file, resulting in the execution of arbitrary code in the context of the current user. (CVE-2015-3788)

- A memory corruption issue exists due to improper validation of user-supplied input when handling 3GPP STSD sample description entry sizes. A remote attacker can exploit this issue by convincing a user to open a specially crafted file, resulting in the execution of arbitrary code in the context of the current user. (CVE-2015-3789)

- A memory corruption issue exists due to improper validation of user-supplied input when handling MVHD atom sizes. A remote attacker can exploit this issue by convincing a user to open a specially crafted file, resulting in the execution of arbitrary code in the context of the current user. (CVE-2015-3790)

- A memory corruption issue exists due to improper validation of user-supplied input when handling mismatching ESDS atom descriptor type lengths. A remote attacker can exploit this issue by convincing a user to open a specially crafted file, resulting in the execution of arbitrary code in the context of the current user. (CVE-2015-3791)

- A memory corruption issue exists due to improper validation of user-supplied input when handling MDAT sections. A remote attacker can exploit this issue by convincing a user to open a specially crafted file, resulting in the execution of arbitrary code in the context of the current user. (CVE-2015-3792)

- An unspecified memory corruption issue exists due to improper validation of user-supplied input. A remote attacker can exploit this issue by convincing a user to open a specially crafted file, resulting in the execution of arbitrary code in the context of the current user. (CVE-2015-5751)

- An unspecified memory corruption issue exists due to improper validation of user-supplied input. A remote attacker can exploit this issue by convincing a user to open a specially crafted file, resulting in the execution of arbitrary code in the context of the current user. (CVE-2015-5779)

- An unspecified memory corruption issue exists due to improper validation of user-supplied input. A remote attacker can exploit this issue by convincing a user to open a specially crafted file, resulting in the execution of arbitrary code in the context of the current user. (CVE-2015-5785)

- An unspecified memory corruption issue exists due to improper validation of user-supplied input. A remote attacker can exploit this issue by convincing a user to open a specially crafted file, resulting in the execution of arbitrary code in the context of the current user. (CVE-2015-5786)

Solution
Upgrade to Apple QuickTime 7.7.8 or later.
Additional Resources
https://support.apple.com/en-us/HT205046
Comments
N/A

Vulnerability	KB5008212: Windows 10 Version 2004 / 20H2 / 21H1 / 21H2 Security Update (December 2021)					
Synopsis	The remote Windows host is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	7.5			**Exploitable**	true	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	192.168.0.1	445	cifs	Desktop23	DESKTOP23	
	192.168.0.1	445	cifs	Desktop31	DESKTOP31	
	192.168.0.1	445	cifs	Desktop30	DESKTOP30	

Description
The remote Windows host is missing security update 5008212. It is, therefore, affected by multiple vulnerabilities: - An elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges. (CVE-2021-41333, CVE-2021-43207, CVE-2021-43223, CVE-2021-43226, CVE-2021-43229, CVE-2021-43230, CVE-2021-43231, CVE-2021-43237, CVE-2021-43238, CVE-2021-43239, CVE-2021-43240, CVE-2021-43247, CVE-2021-43248, CVE-2021-43883, CVE-2021-43893) - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2021-43215, CVE-2021-43217, CVE-2021-43232, CVE-2021-43233, CVE-2021-43234) - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2021-43216, CVE-2021-43222, CVE-2021-43224, CVE-2021-43227, CVE-2021-43235, CVE-2021-43236, CVE-2021-43244) - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2021-43219, CVE-2021-43228, CVE-2021-43246)
Solution
Apply Cumulative Update KB5008212.
Additional Resources
https://support.microsoft.com/en-us/help/5008212
Comments
N/A

Vulnerability	SNMP Agent Default Community Name (public)					
Synopsis	The community name of the remote SNMP server can be guessed.					
Severity	High					
CVSS Score	7.5			**Exploitable**	false	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
	192.168.0.1	161	snmp			
Description						
It is possible to obtain the default community name of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).						
Solution						
Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.						
Additional Resources						
Comments						
N/A						

Vulnerability	Apple iTunes < 12.12.3 Multiple Vulnerabilities (credentialed check)					
Synopsis	An application installed on the remote host is affected by multiple vulnerabilities					
Severity	High					
CVSS Score	7.5			Exploitable	false	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop30	DESKTOP30	

Description

The version of Apple iTunes installed on the remote Windows host is prior to 12.12.3. It is, therefore, affected by multiple vulnerabilities as referenced in the HT213188 advisory.

- Processing a maliciously crafted image may lead to arbitrary code execution (CVE-2022-22611)

- Processing a maliciously crafted image may lead to heap corruption (CVE-2022-22612)

- Processing maliciously crafted web content may disclose sensitive user information (CVE-2022-22662)

- Processing maliciously crafted web content may lead to arbitrary code execution (CVE-2022-22629)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apple iTunes version 12.12.3 or later.

Additional Resources

https://support.apple.com/en-us/HT213188

Comments

N/A

Vulnerability	Windows Security Feature Bypass in Secure Boot (BootHole)					
Synopsis	The remote Windows host is affected by multiple vulnerabilities.					
Severity	High					
CVSS Score	7.2			Exploitable		
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop19	DESKTOP19	
	192.168.0.1	445	cifs	Desktop20	DESKTOP20	

Description

The remote Windows host is missing an update to the Secure Boot DBX. It is, therefore, affected by multiple vulnerabilities:

- A flaw was found in grub2 in versions prior to 2.06. The rmmod implementation allows the unloading of a module used as a dependency without checking if any other dependent module is still loaded leading to a use-after-free scenario. This could allow arbitrary code to be executed or a bypass of Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. (CVE-2020-25632)

- A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. (CVE-

2021-20233)
Additionally, the host is affected by several other security feature bypasses in Secure Boot.
Note: Tenable is testing for the presence of the expected signatures added in the March 2021 DBX update referenced in the vendor advisory.

Solution

Refer to the vendor advisory for guidance.

Additional Resources

http://www.nessus.org/u?6f75665a
http://www.nessus.org/u?840ba26f

Comments

N/A

Vulnerability	Insecure Windows Service Permissions					
Synopsis	At least one improperly configured Windows service may have a privilege escalation vulnerability.					
Severity	High					
CVSS Score	7.2		Exploitable			
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
	192.168.0.1	445	cifs	Desktop24	DESKTOP24	

Description

At least one Windows service executable with insecure permissions was detected on the remote host. Services configured to use an executable with weak permissions are vulnerable to privilege escalation attacks. An unprivileged user could modify or overwrite the executable with arbitrary code, which would be executed the next time the service is started. Depending on the user that the service runs as, this could result in privilege escalation.

This plugin checks if any of the following groups have permissions to modify executable files that are started by Windows services :

- Everyone
- Users
- Domain Users
- Authenticated Users

Solution

Ensure the groups listed above do not have permissions to modify or write service executables. Additionally, ensure these groups do not have Full Control permission to any directories that contain service executables.

Additional Resources

http://www.nessus.org/u?e4e766b2

Comments

N/A