centrexIT

SQ1Shield

VULNERABILITY ASSESSMENT

Security Assessment Technical Report

8th May 2023 Version 1.0

Table Of Contents

Confidentiality Statement

This document is the exclusive property of CentrexIT and Secqureone. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both CentrexIT and Secqureone. CentrexIT may share this document with auditors under non-disclosure agreements to demonstrate Vulnerability Assessment requirement compliance.

Disclaimer

A Vulnerability Assessment is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Secqureone prioritized the assessment to identify the weakest security controls. Secqureone recommends conducting similar assessments on an annual basis by External or third-party assessors to ensure the continued success of the controls.

SecqureOne Vulnerability Assessment: Methodology

1. Identifying the scope

The assets on which Vulnerability Assessment should be performed are identified by the client. The assets are validated and necessary access and credentials are obtained by SecqureOne to perform VA.

2. Vulnerabilities detection

For Vulnerability Assessment, access to the network as well as credentials are required as SecqureOne will be conducting a credentialed Vulnerability Assessment. SecqureOne will be using an automated tool which will do a credentialed assessment through SMB for windows-based OS and SSH for Linux based OS.

3. Controls evaluated

Through credentialed assessments, the following controls are evaluated for vulnerability assessment.

- Missing security patches
- Missing security OS updates
- Vulnerable configurations in the OS
- Vulnerable version of installed applications
- Vulnerable configurations of the installed applications
- Vulnerable encryptions used in the scoped assets

4. Vulnerable encryptions used in the scoped assets

The vulnerabilities identified through VA are analysed further by the team to weed out false positives and to validate the criticality of the identified vulnerabilities. The team will further provide suggestions to patch or mitigate the identified vulnerabilities.

5. Reporting

Based on the analysis, SecqureOne will provide a PDF report to the client, with details of the identified vulnerabilities which will include the description, severity and suggestions to patch or mitigate the vulnerabilities.

Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window.

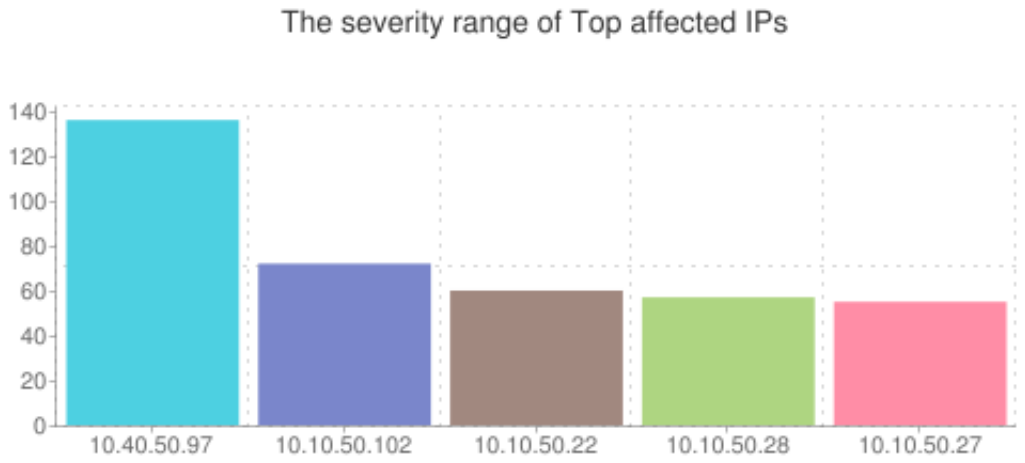
Summary of Findings

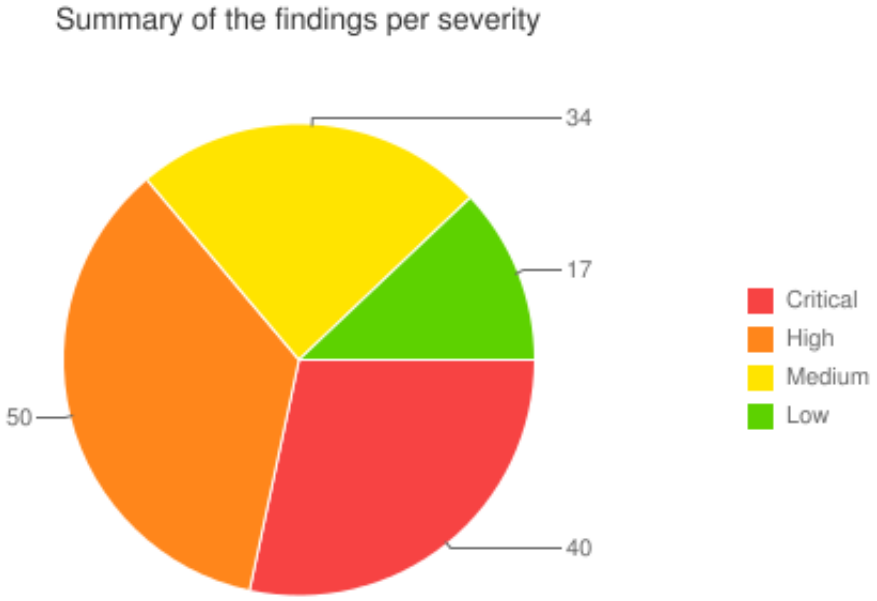
In this assessment, all 300 hosts identified as belonging to the CentrexIT domain and were successfully scanned.

39	50	33	13
Critical	High	Medium	Low

Graphical representation of findings

The table below provides a summary of the findings per severity





Vulnerability Summary

Finding	Severity	Status	
Vulnerability Assessment findings		**Fixed**	**Pending**
Mozilla Firefox Less-than 94.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	**Critical**	**1**	**0**
Mozilla Firefox Less-than 96.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	**Critical**	**1**	**0**
ASP.NET Core SEoL: An unsupported version of ASP.NET Core is installed on the remote host.	**Critical**	**0**	**1**
Microsoft .NET Core SEoL: An unsupported version of Microsoft .NET Core is installed on the remote host.	**Critical**	**1**	**0**
Microsoft Office 365 Unsupported Channel Version Detection: The remote host contains an unsupported Channel version of Microsoft Office 365.	**Critical**	**0**	**1**
Mozilla Foundation Unsupported Application Detection: The remote host contains one or more unsupported applications from the Mozilla Foundation.	**Critical**	**3**	**0**
Microsoft SQL Server Unsupported Version Detection: An unsupported version of a database server is running on the remote host.	**Critical**	**1**	**0**
Microsoft SQL Server Unsupported Version Detection (remote check): An unsupported version of a database server is running on the remote host.	**Critical**	**0**	**1**
Apache Log4j Unsupported Version Detection: A logging library running on the remote host is no longer supported.	**Critical**	**1**	**1**
Mozilla Firefox Less-than 93.0: A web browser installed on the remote Windows host is affected by multiple	**Critical**	**0**	**1**

vulnerabilities.			
Mozilla Firefox Less-than 95.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
Mozilla Firefox Less-than 100.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
Mozilla Firefox Less-than 101.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
Mozilla Firefox Less-than 102.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
Mozilla Firefox Less-than 103.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	1	0
KB5023697: Windows 10 Version 1607 and Windows Server 2016 Security Update (March 2023): The remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
KB5025230: Windows 2022 / Azure Stack HCI 22H2 Security Update (April 2023): The remote Windows host is affected by multiple vulnerabilities.	Critical	0	3
KB5025272: Windows Server 2012 Security Update (April 2023): The remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
KB5025228: Windows 10 Version 1607 and Windows Server 2016 Security Update (April 2023): The remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
SSL Version 2 and 3 Protocol Detection: The remote service encrypts traffic using a protocol with known weaknesses.	Critical	2	1

Microsoft Edge (Chromium) Less-than 111.0.1661.54 / 110.0.1587.78 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.	Critical	2	2
Google Chrome Less-than 112.0.5615.49 Multiple Vulnerabilities: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	7	0
KB4025339: Windows 10 Version 1607 and Windows Server 2016 July 2017 Cumulative Update: The remote Windows host is affected by multiple vulnerabilities.	Critical	1	1
Mozilla Firefox Less-than 109.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	1	2
Mozilla Firefox Less-than 110.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	0	3
Mozilla Firefox Less-than 111.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	0	3
JBoss Enterprise Application Platform doFilter() Method Insecure Deserialization RCE: The remote host is affected by a remote code execution vulnerability.	Critical	1	1
KB5022895: Windows Server 2012 Security Update (February 2023): The remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
KB5023752: Windows Server 2012 Security Update (March 2023): The remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
Apache Log4j 1.x Multiple Vulnerabilities: A logging library running on the remote host has multiple vulnerabilities.	Critical	0	2

Oracle Java SE 1.7.0_241 / 1.8.0_231 / 1.11.0_5 / 1.13.0_1 Multiple Vulnerabilities (Oct 2019 CPU) (Windows): The remote Windows host contains a programming platform that is affected by multiple vulnerabilities.	Critical	0	1
Mozilla Firefox Less-than 107.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	0	2
Microsoft Silverlight Unsupported Version Detection (Windows): The remote host has an unsupported version of Microsoft Silverlight.	Critical	0	1
PuTTY Less-than 0.71 Multiple Vulnerabilities: The remote Windows host has an SSH client that is affected by multiple vulnerabilities.	Critical	0	1
Mozilla Firefox Less-than 90.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
Mozilla Firefox Less-than 97.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
Mozilla Firefox Less-than 97.0.2: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
Mozilla Firefox Less-than 98.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	Critical	0	1
Foxit PDF Reader Less-than 12.1.2 Multiple Vulnerabilities: A PDF viewer installed on the remote Windows host is affected by multiple vulnerabilities	Critical	0	1
Oracle Java SE 1.7.0_221 / 1.8.0_211 / 1.11.0_3 / 1.12.0_1 Multiple Vulnerabilities (Apr 2019 CPU): The	Critical	1	0

remote Windows host contains a programming platform that is affected by multiple vulnerabilities.			
Security Updates for Microsoft .NET core (March 2022): The Microsoft .NET core installations on the remote host are affected by multiple vulnerabilities.	High	0	1
Mozilla Firefox Less-than 99.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	1
Mozilla Firefox Less-than 100.0.2: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	1
Mozilla Firefox Less-than 104.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	1
Mozilla Firefox Less-than 105.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	1
Mozilla Firefox Less-than 106.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	1
Security Updates for Microsoft .NET Core (December 2022): The Microsoft .NET core installations on the remote host are affected by remote code execution vulnerability.	High	0	1
Security Updates for Microsoft ASP.NET Core (December 2022): The Microsoft ASP.NET core installations on the remote host are affected by remote code execution vulnerability.	High	0	1
Microsoft Edge (Chromium) Less-than 112.0.1722.48 : The remote host has an web browser installed that is affected by a vulnerability.	High	0	4

Microsoft Edge (Chromium) Less-than 112.0.1722.58 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.	High	0	4
Microsoft Edge (Chromium) Less-than 111.0.1661.41 / 110.0.1587.69 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.	High	0	4
Microsoft Edge (Chromium) Less-than 110.0.1587.41 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.	High	0	2
Microsoft Edge (Chromium) Less-than 110.0.1587.56 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.	High	0	2
Security Updates for Microsoft SQL Server (February 2023): The Microsoft SQL Server installation on the remote host is affected by multiple vulnerabilities.	High	0	1
Mozilla Firefox Less-than 108.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	2
Mozilla Firefox Less-than 89.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	1
Mozilla Firefox Less-than 91.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	1
Mozilla Firefox Less-than 92.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	1

Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU): The remote host is affected by multiple vulnerabilities.	High	0	2
Insecure Windows Service Permissions: At least one improperly configured Windows service may have a privilege escalation vulnerability.	High	0	2
Oracle Java SE 1.7.0_261 / 1.8.0_251 / 1.11.0_7 / 1.14.0_1 Multiple Vulnerabilities (Apr 2020 CPU): The remote host is affected by multiple vulnerabilities	High	0	1
Oracle Java SE 1.7.0_271 / 1.8.0_261 / 1.11.0_8 / 1.14.0_2 Multiple Vulnerabilities (Jul 2020 CPU): The remote host is affected by multiple vulnerabilities	High	0	1
Windows Security Feature Bypass in Secure Boot (BootHole): The remote Windows host is affected by multiple vulnerabilities.	High	0	1
Oracle Java SE 1.7.0_251 / 1.8.0_241 / 1.11.0_6 / 1.13.0_2 Multiple Vulnerabilities (Jan 2020 CPU): The remote Windows host contains a programming platform that is affected by multiple vulnerabilities.	High	0	1
Mozilla Firefox Less-than 89.0.1: A web browser installed on the remote Windows host is affected by a vulnerability.	High	0	1
Mozilla Firefox Less-than 91.0.1: A web browser installed on the remote Windows host is affected by a vulnerability.	High	0	1
Security Updates for Microsoft ASP.NET Core (December 2021): The Microsoft ASP.NET Core installations on the remote host are missing a security update.	High	0	1
Security Updates for Microsoft .NET Core (October 2022): The Microsoft .NET core installations on the	High	0	1

remote host are affected by a privilege escalation vulnerability.			
Adobe Reader Less-than 20.005.30467 / 23.001.20143 Multiple Vulnerabilities (APSB23-24): The version of Adobe Reader installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	1
Oracle Java SE Multiple Vulnerabilities (April 2023 CPU): The remote host is affected by multiple vulnerabilities.	High	0	4
Adobe Reader Less-than 20.005.30407 / 22.003.20258 Multiple Vulnerabilities (APSB22-46): The version of Adobe Reader installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	1
Adobe Reader Less-than 20.005.30436 / 22.003.20310 Multiple Vulnerabilities (APSB23-01): The version of Adobe Reader installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	1
Microsoft Windows Unquoted Service Path Enumeration: The remote Windows host has at least one service installed that uses an unquoted service path.	High	0	5
Security Updates for Microsoft .NET Framework (February 2023): The Microsoft .NET Framework installation on the remote host is missing a security update.	High	0	1
Microsoft Teams Less-than 1.3.0.13000 Remote Code Execution: The version of Microsoft Teams installed on the remote Windows host is affected by a remote code execution vulnerability.	High	0	1
Security Updates for Microsoft .NET core (May 2022): The Microsoft .NET core installations on the remote host are affected by multiple vulnerabilities.	High	0	1

Security Updates for Microsoft ASP.NET Core (September 2022): The Microsoft ASP.NET Core installations on the remote host are missing a security update.	High	0	1
Security Updates for Microsoft .NET Core (September 2022): The Microsoft .NET core installations on the remote host are affected by a denial of service vulnerability.	High	0	1
DNS Server Spoofed Request Amplification DDoS: The remote DNS server could be used in a distributed denial of service attack.	High	0	3
Mozilla Firefox Less-than 112.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.	High	0	3
SSL Certificate Signed Using Weak Hashing Algorithm: An SSL certificate in the certificate chain has been signed using a weak hash algorithm.	High	0	10
SSL Medium Strength Cipher Suites Supported (SWEET32): The remote service supports the use of medium strength SSL ciphers.	High	0	27
Oracle Java SE 1.7.0_311 / 1.8.0_301 / 1.11.0_12 / 1.16.0_2 Multiple Vulnerabilities (July 2021 CPU): The remote host is affected by multiple vulnerabilities.	High	0	2
Oracle Java SE Multiple Vulnerabilities (April 2022 CPU): The remote host is affected by multiple vulnerabilities.	High	0	2
Oracle Java SE Multiple Vulnerabilities (July 2022 CPU): The remote host is affected by multiple vulnerabilities.	High	0	2
Security Updates for Internet Explorer (September 2017): The Internet Explorer installation on the remote	High	0	3

host is affected by multiple vulnerabilities.			
Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104): A package installed on the remote host is affected by a remote code execution vulnerability.	High	0	2
Security Update for .NET Core (August 2021): The remote Windows host is affected by a .NET Core denial of service (DoS) vulnerability.	High	0	1
WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck): The remote Windows host is potentially missing a mitigation for a remote code execution vulnerability.	High	0	21
Untrusted Microsoft Office Macro Execution Enabled: A Microsoft Office application installed on the remote host has untrusted macro execution settings enabled.	High	0	1
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE): It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.	Medium	0	3
SSL Certificate Cannot Be Trusted: The SSL certificate for this service cannot be trusted.	Medium	0	26
SSL Self-Signed Certificate: The SSL certificate chain for this service ends in an unrecognized self-signed certificate.	Medium	0	23
TLS Version 1.0 Protocol Detection: The remote service encrypts traffic using an older version of TLS.	Medium	0	27
TLS Version 1.1 Protocol Deprecated: The remote service encrypts traffic using an older version of TLS.	Medium	0	28
Windows Speculative Execution Configuration Check: The remote host has not properly mitigated a series of speculative execution vulnerabilities.	Medium	0	16

Windows 10 / Windows Server 2016 September 2017 Information Disclosure Vulnerability (CVE-2017-8529): The remote Windows host is affected by an information disclosure vulnerability.	Medium	0	12
HSTS Missing From HTTPS Server (RFC 6797): The remote web server is not enforcing HSTS, as defined by RFC 6797.	Medium	0	5
Remote Desktop Protocol Server Man-in-the-Middle Weakness: It may be possible to get access to the remote host.	Medium	0	6
Security Updates for Microsoft SQL Server Reporting Services (September 2020): The Microsoft SQL Server Reporting Services installation on the remote host is missing a security update.	Medium	0	2
Microsoft Edge (Chromium) Less-than 112.0.1722.34 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.	Medium	0	4
JQuery 1.2 Less-than 3.5.0 Multiple XSS: The remote web server is affected by multiple cross site scripting vulnerability.	Medium	0	2
Security Updates for Microsoft .NET Core (August 2022): The Microsoft .NET core installations on the remote host are affected by a spoofing vulnerability.	Medium	0	1
SSL RC4 Cipher Suites Supported (Bar Mitzvah): The remote service supports the use of the RC4 cipher.	Medium	0	15
Curl Use-After-Free Less-than 7.87 (CVE-2022-43552): The remote Windows host has a program that is affected by a use-after-free vulnerability.	Medium	3	3
Oracle Java SE 1.7.0_301 / 1.8.0_291 / 1.11.0_11 / 1.16.0_1 Multiple Vulnerabilities (Apr 2021 CPU): The	Medium	0	2

remote host is affected by multiple vulnerabilities.			
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption): The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.	Medium	0	1
VMware vSphere Client XXE Injection Information Disclosure (VMSA-2016-0022): The remote host has a virtualization client application installed that is affected by an information disclosure vulnerability.	Medium	0	1
Potentially Dangerous PATH Variables: Potentially dangerous PATH variables are present in the PATH of the remote host.	Medium	1	0
ADV180002: Microsoft SQL Server January 2018 Security Update (Meltdown) (Spectre): The remote SQL server is affected by multiple vulnerabilities.	Medium	0	2
Security Updates for Microsoft .NET core (June 2022): The Microsoft .NET core installations on the remote host are affected by an information disclosure vulnerability.	Medium	0	1
Security Updates for SQL Server Management Studio (August 2020): The SQL Server Management Studio installation on the remote host is missing a security update.	Medium	0	2
Security Update for Microsoft ASP.NET Core (August 2021): The Microsoft ASP.NET Core installations on the remote host is affected by multiple vulnerabilities.	Medium	0	1
SSL Certificate with Wrong Hostname: The SSL certificate for this service is for a different host.	Medium	0	12
SMB Signing not required: Signing is not required on the remote SMB server.	Medium	1	33

SSL Certificate Expiry: The remote server's SSL certificate has already expired.	Medium	0	1
Oracle Java SE 1.7.0_281 / 1.8.0_271 / 1.11.0_9 / 1.15.0_1 Multiple Vulnerabilities (Oct 2020 CPU): The remote host is affected by multiple vulnerabilities	Medium	0	2
Oracle Java SE 1.7.0_291 / 1.8.0_281 / 1.11.0_10 / 1.15.0_2 Information Disclosure (Windows Jan 2021 CPU): The remote host is affected by an information disclosure vulnerability.	Medium	0	2
Oracle Java SE 1.7.0_331 / 1.8.0_321 / 1.11.0_14 / 1.17.0_2 Multiple Vulnerabilities (January 2022 CPU): The remote host is affected by multiple vulnerabilities.	Medium	0	2
Oracle Java SE Multiple Vulnerabilities (October 2022 CPU): The remote host is affected by multiple vulnerabilities.	Medium	0	2
Oracle Java SE Multiple Vulnerabilities (January 2023 CPU): The remote host is affected by multiple vulnerabilities.	Medium	0	4
Oracle Java SE 1.7.0_231 / 1.8.0_221 / 1.11.0_4 / 1.12.0_2 Multiple Vulnerabilities (Jul 2019 CPU): The remote Windows host contains a programming platform that is affected by multiple vulnerabilities.	Medium	0	1
SSL Weak Cipher Suites Supported: The remote service supports the use of weak SSL ciphers.	Medium	0	1
Terminal Services Doesn't Use Network Level Authentication (NLA) Only: The remote Terminal Services doesn't use Network Level Authentication only.	Medium	0	8
Oracle Java SE 1.7.x Less-than 1.7.0_211 / 1.8.x Less-than 1.8.0_201 / 1.11.x Less-than 1.11.0_2 Multiple Vulnerabilities (January 2019 CPU): The remote Windows host contains a programming platform that is	Low	0	1

affected by multiple vulnerabilities.			
SSH Weak Key Exchange Algorithms Enabled: The remote SSH server is configured to allow weak key exchange algorithms.	Low	1	0
VMware Tools 10.x / 11.x / 12.x Less-than 12.1.5 DoS (VMSA-2022-0029): A virtualization tool suite is installed on the remote Windows host is affected by a denial of service vulnerability.	Low	0	1
MS15-124: Cumulative Security Update for Internet Explorer (CVE-2015-6161) (3125869): The remote host has a web browser installed that is affected by multiple vulnerabilities.	Low	0	3
DNS Server Recursive Query Cache Poisoning Weakness: The remote name server allows recursive queries to be performed by the host running nessusd.	Low	0	3
Windows Defender Antimalware/Antivirus Signature Definition Check: Windows Defender AntiMalware / AntiVirus Signatures are continuously not and should not be more than 1 day old	Low	0	1
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits: The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.	Low	0	6
DNS Server Zone Transfer Information Disclosure (AXFR): The remote name server allows zone transfers	Low	0	2
Microsoft Windows LM / NTLMv1 Authentication Enabled: The remote Windows host is configured to use an insecure authentication protocol.	Low	0	2
Terminal Services Encryption Level is not FIPS-140 Compliant: The remote host is not FIPS-140 compliant.	Low	0	6

Terminal Services Encryption Level is Medium or Low: The remote host is using weak cryptography.	Low	0	6
Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities: The remote web server is affected by multiple vulnerabilities.	Low	0	2
MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483): The remote Windows host is affected by a remote code execution vulnerability.	Low	0	3
MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE): The remote host is affected by a remote information disclosure vulnerability.	Low	0	1
SSH Server CBC Mode Ciphers Enabled: The SSH server is configured to use Cipher Block Chaining.	Low	1	0
SSH Weak MAC Algorithms Enabled: The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.	Low	1	0
SSH Weak Algorithms Supported: The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.	Low	1	0

Technical Findings

1. Mozilla Firefox Less-than 94.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Closed

Description

The version of Firefox installed on the remote Windows host is prior to 94.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-48 advisory. - The iframe sandbox rules were not correctly applied to XSLT stylesheets, allowing an iframe to bypass restrictions such as executing scripts or navigating the top-level frame. (CVE-2021-38503) - When interacting with an HTML input element's file picker dialog with Less-thancodeGreater-thanwebkitdirectoryLess-than/codeGreater-than set, a use-after-free could have resulted, leading to memory corruption and a potentially exploitable crash. (CVE-2021-38504) - Microsoft introduced a new feature in Windows 10 known as Cloud Clipboard which, if enabled, will record data copied to the clipboard to the cloud, and make it available on other computers in certain scenarios. Applications that wish to prevent copied data from being recorded in Cloud History must use specific clipboard formats; and Firefox before versions 94 and ESR 91.3 did not implement them. This could have caused sensitive data to be recorded to a user's Microsoft account. This bug only affects Firefox for Windows 10+ with Cloud Clipboard enabled. Other operating systems are unaffected. (CVE-2021-38505) - Through a series of navigations, Firefox could have entered fullscreen mode without notification or warning to the user. This could lead to spoofing attacks on the browser UI including phishing. (CVE-2021-38506) - The Opportunistic Encryption feature of HTTP2 (RFC 8164) allows a connection to be transparently upgraded to TLS while retaining the visual properties of an HTTP connection, including being same-origin with unencrypted connections on port 80. However, if a second encrypted port on the same IP address (e.g. port 8443) did not opt-in to opportunistic encryption; a network attacker could forward a connection from the browser to port 443 to port 8443, causing the browser to treat the content of port 8443 as same-origin with HTTP. This was resolved by disabling the Opportunistic Encryption feature, which had low usage. (CVE-2021-38507) - By displaying a form validity message in the correct location at the same time as a permission prompt (such as for geolocation), the validity message could have obscured the prompt, resulting in the user potentially being tricked into granting the permission. (CVE-2021-38508) - Due to an unusual sequence of attacker-controlled events, a

Javascript Less-thancodeGreater-thanalert()Less-than/codeGreater-than dialog with arbitrary (although unstyled) contents could be displayed over top an uncontrolled webpage of the attacker's choosing. (CVE-2021-38509) - The executable file warning was not presented when downloading .inetloc files, which can run commands on a user's computer. Note: This issue only affected Mac OS operating systems. Other operating systems are unaffected. (CVE-2021-38510) 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 Mozilla Firefox version 94.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2021-48/

2. Mozilla Firefox Less-than 96.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Closed

Description

The version of Firefox installed on the remote Windows host is prior to 96.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-01 advisory. - A race condition could have allowed bypassing the fullscreen notification which could have lead to a fullscreen window spoof being unnoticed. This bug only affects Firefox for Windows. Other operating systems are unaffected. (CVE-2022-22746) - When navigating from inside an iframe while requesting fullscreen access, an attacker-controlled tab could have made the browser unable to leave fullscreen mode. (CVE-2022-22743) - When inserting text while in edit mode, some characters might have lead to out-of-bounds memory access causing a potentially exploitable crash. (CVE-2022-22742) - When resizing a popup while requesting fullscreen access, the popup would have become unable to leave fullscreen mode. (CVE-2022-22741) - Certain network request objects were freed too early when releasing a network request handle. This could have lead to a use-after-free causing a potentially exploitable crash. (CVE-2022-22740) - Applying a CSS filter effect could have accessed out of bounds memory. This could have lead to a heap- buffer-overflow causing a potentially exploitable crash. (CVE-2022-22738) - Constructing audio sinks could have lead to a race condition when playing audio files and closing windows. This could have lead to a use-after-free causing a potentially exploitable crash. (CVE-2022-22737) - It was possible to construct specific XSLT markup that would be able to

bypass an iframe sandbox. (CVE-2021-4140) - By generally accepting and passing resource handles across processes, a compromised content process might have confused higher privileged processes to interact with handles that the unprivileged process should not have access to. This bug only affects Firefox for Windows and MacOS. Other operating systems are unaffected. (CVE-2022-22750) - When scanning QR codes, Firefox for Android would have allowed navigation to some URLs that do not point to web content. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2022-22749) - Malicious websites could have confused Firefox into showing the wrong origin when asking to launch a program and handling an external URL protocol. (CVE-2022-22748) - Securitypolicyviolation events could have leaked cross-origin information for frame-ancestors violations (CVE-2022-22745) - The constructed curl command from the Copy as curl feature in DevTools was not properly escaped for PowerShell. This could have lead to command injection if pasted into a Powershell prompt. This bug only affects Firefox for Windows. Other operating systems are unaffected. (CVE-2022-22744) - After accepting an untrusted certificate, handling an empty pkcs7 sequence as part of the certificate data could have lead to a crash. This crash is believed to be unexploitable. (CVE-2022-22747) - If Firefox was installed to a world-writable directory, a local privilege escalation could occur when Firefox searched the current directory for system libraries. However the install directory is not world- writable by default. This bug only affects Firefox for Windows in a non-default installation. Other operating systems are unaffected. (CVE-2022-22736) - Malicious websites could have tricked users into accepting launching a program to handle an external URL protocol. (CVE-2022-22739) - Mozilla developers Calixte Denizet, Kershaw Chang, Christian Holler, Jason Kratzer, Gabriele Svelto, Tyson Smith, Simon Giesecke, and Steve Fink reported memory safety bugs present in Firefox 95 and Firefox ESR 91.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-22751) - Mozilla developers Christian Holler and Jason Kratzer reported memory safety bugs present in Firefox 95. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-22752) 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 Mozilla Firefox version 96.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-01/

3. ASP.NET Core SEoL: An unsupported version of ASP.NET Core is installed on the remote host.

Severity	**Critical**	Status	**Open**
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

According to its version, the ASP.NET Core installed on the remote host is no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of ASP.NET Core that is currently supported.
http://www.nessus.org/u?89faa62b

4. Microsoft .NET Core SEoL: An unsupported version of Microsoft .NET Core is installed on the remote host.

Severity	Critical	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Closed

Description

According to its version, the Microsoft .NET Core installed on the remote host is no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Microsoft .NET Core that is currently supported.
http://www.nessus.org/u?89faa62b

5. Microsoft Office 365 Unsupported Channel Version Detection: The remote host contains an unsupported Channel version of Microsoft Office 365.

Severity	Critical	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

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

6. Mozilla Foundation Unsupported Application Detection: The remote host contains one or more unsupported applications from the Mozilla Foundation.

Severity	Critical	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Closed

LWDC-VEEAM - (10.10.50.102) - Closed

CIT-TECH - (10.40.50.97) - Closed

Description

According to its version, there is at least one unsupported Mozilla application (Firefox, Thunderbird, and/or SeaMonkey) installed on the remote host. This version of the software is no longer actively maintained. 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 that is currently supported. https://www.mozilla.org/en-US/firefox/organizations/faq/ https://www.mozilla.org/en-US/security/known-vulnerabilities/ https://www.mozilla.org/en-US/firefox/new/ https://www.mozilla.org/en-US/thunderbird/ https://www.seamonkey-project.org/releases/

7. Microsoft SQL Server Unsupported Version Detection: An unsupported version of a database server is running on the remote host.

Severity	**Critical**	Status	**Closed**
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CITS8 - (10.10.50.28) - Closed

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

8. Microsoft SQL Server Unsupported Version Detection (remote check): An unsupported version of a database server is running on the remote host.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS8 - (10.10.50.28) - Open

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

9. Apache Log4j Unsupported Version Detection: A logging library running on the remote host is no longer supported.

Severity	Critical	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

CIT-FS - (10.10.50.30) - Closed

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.

http://www.nessus.org/u?59f655a2

10. Mozilla Firefox Less-than 93.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 93.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-43 advisory. - During operations on MessageTasks, a task may have been removed while it was still scheduled, resulting in memory corruption and a potentially exploitable crash. (CVE-2021-38496) - Through use of reportValidity() and window.open(), a plain-text validation message could have been overlaid on another origin, leading to possible user confusion and spoofing attacks. (CVE-2021-38497) - During process shutdown, a document could have caused a use-after-free of a languages service object, leading to memory corruption and a potentially exploitable crash. (CVE-2021-38498) - In the crossbeam crate, one or more tasks in the worker queue could have been be popped twice instead of other tasks that are forgotten and never popped. If tasks are allocated on the heap, this could have caused a double free and a memory leak. (CVE-2021-32810) - Mozilla developers and community members Andreas Pehrson and Christian Holler reported memory safety bugs present in Firefox 92 and Firefox ESR

91.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-38500) - Mozilla developers and community members Kevin Brosnan, Mihai Alexandru Michis, and Christian Holler reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-38501) - Mozilla developers and community members Julien Cristau, Christian Holler reported memory safety bugs present in Firefox 92. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-38499) 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 Mozilla Firefox version 93.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2021-43/

11. Mozilla Firefox Less-than 95.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	**Critical**	Status	**Open**
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 95.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-52 advisory. - Under certain circumstances, asynchronous functions could have caused a navigation to fail but expose the target URL. (CVE-2021-43536) - An incorrect type conversion of sizes from 64bit to 32bit integers allowed an attacker to corrupt memory leading to a potentially exploitable crash. (CVE-2021-43537) - By misusing a race in our notification code, an attacker could have forcefully hidden the notification for pages that had received full screen and pointer lock access, which could have been used for spoofing attacks. (CVE-2021-43538) - Failure to correctly record the location of live pointers across wasm instance calls resulted in a GC occurring within the call not tracing those live pointers. This could have led to a use-after-free causing a potentially exploitable crash. (CVE-2021-43539) - WebExtensions with the correct permissions were able to create and install ServiceWorkers for third-party websites that would not have been uninstalled with the extension. (CVE-2021-43540) - When invoking protocol

handlers for external protocols, a supplied parameter URL containing spaces was not properly escaped. (CVE-2021-43541) - Using XMLHttpRequest, an attacker could have identified installed applications by probing error messages for loading external protocols. (CVE-2021-43542) - Documents loaded with the CSP sandbox directive could have escaped the sandbox's script restriction by embedding additional content. (CVE-2021-43543) - When receiving a URL through a SEND intent, Firefox would have searched for the text, but subsequent usages of the address bar might have caused the URL to load unintentionally, which could lead to XSS and spoofing attacks. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-43544) - Using the Location API in a loop could have caused severe application hangs and crashes. (CVE-2021-43545) - It was possible to recreate previous cursor spoofing attacks against users with a zoomed native cursor. (CVE-2021-43546) 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 Mozilla Firefox version 95.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2021-52/

12. Mozilla Firefox Less-than 100.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 100.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-16 advisory. - When reusing existing popups Firefox would have allowed them to cover the fullscreen notification UI, which could have enabled browser spoofing attacks. (CVE-2022-29914) - Documents in deeply-nested cross-origin browsing contexts could have obtained permissions granted to the top-level origin, bypassing the existing prompt and wrongfully inheriting the top-level permissions. (CVE-2022-29909) - Firefox behaved slightly differently for already known resources when loading CSS resources involving CSS variables. This could have been used to probe the browser history. (CVE-2022-29916) - Firefox did not properly protect against top-level navigations for an iframe sandbox with a policy relaxed through a keyword like Less-thancodeGreater-thanallow-top-navigation-by-user-activationLess-than/codeGreater-than.

(CVE-2022-29911) - Requests initiated through reader mode did not properly omit cookies with a SameSite attribute. (CVE-2022-29912) - When closed or sent to the background, Firefox for Android would not properly record and persist HSTS settings. Note: This issue only affected Firefox for Android. Other operating systems are unaffected. (CVE-2022-29910) - The Performance API did not properly hide the fact whether a request cross-origin resource has observed redirects. (CVE-2022-29915) - Mozilla developers Andrew McCreight, Gabriele Svelto, Tom Ritter and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 99 and Firefox ESR 91.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-29917) - Mozilla developers Gabriele Svelto, Randell Jesup and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 99. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-29918) 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 Mozilla Firefox version 100.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-16/

13. Mozilla Firefox Less-than 101.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	**Critical**	Status	**Open**
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 101.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-20 advisory. - A malicious website could have learned the size of a cross-origin resource that supported Range requests. (CVE-2022-31736) - A malicious webpage could have caused an out-of-bounds write in WebGL, leading to memory corruption and a potentially exploitable crash. (CVE-2022-31737) - When exiting fullscreen mode, an iframe could have confused the browser about the current state of fullscreen, resulting in potential user confusion or spoofing attacks. (CVE-2022-31738) - When downloading files on Windows, the % character was not escaped, which could have lead to a download incorrectly being saved to attacker-

influenced paths that used variables such as %HOMEPATH% or %APPDATA%. This bug only affects Firefox for Windows. Other operating systems are unaffected. (CVE-2022-31739) - On arm64, WASM code could have resulted in incorrect assembly generation leading to a register allocation problem, and a potentially exploitable crash. (CVE-2022-31740) - A crafted CMS message could have been processed incorrectly, leading to an invalid memory read, and potentially further memory corruption. (CVE-2022-31741) - An attacker could have exploited a timing attack by sending a large number of allowCredential entries and detecting the difference between invalid key handles and cross-origin key handles. This could have led to cross-origin account linking in violation of WebAuthn goals. (CVE-2022-31742) - Firefox's HTML parser did not correctly interpret HTML comment tags, resulting in an incongruity with other browsers. This could have been used to escape HTML comments on pages that put user-controlled data in them. (CVE-2022-31743) - An attacker could have injected CSS into stylesheets accessible via internal URIs, such as resource:, and in doing so bypass a page's Content Security Policy. (CVE-2022-31744) - If array shift operations are not used, the Garbage Collector may have become confused about valid objects. (CVE-2022-31745) - An attacker could have caused an uninitialized variable on the stack to be mistakenly freed, causing a potentially exploitable crash. (CVE-2022-1919) - Mozilla developers Andrew McCreight, Nicolas B. Pierron, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 100 and Firefox ESR 91.9. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-31747) - Mozilla developers Gabriele Svelto, Timothy Nikkel, Randell Jesup, Jon Coppeard, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 100. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-31748) 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 Mozilla Firefox version 101.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/

14. Mozilla Firefox Less-than 102.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	**Critical**	Status	**Open**
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 102.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-24 advisory. - A malicious website that could create a popup could have resized the popup to overlay the address bar with its own content, resulting in potential user confusion or spoofing attacks. This bug only affects Firefox for Linux. Other operating systems are unaffected. (CVE-2022-34479) - Navigations between XML documents may have led to a use-after-free and potentially exploitable crash. (CVE-2022-34470) - An iframe that was not permitted to run scripts could do so if the user clicked on a Less-thancodeGreater-thanjavascript:Less-than/codeGreater-than link. (CVE-2022-34468) - An attacker who could have convinced a user to drag and drop an image to a filesystem could have manipulated the resulting filename to contain an executable extension, and by extension potentially tricked the user into executing malicious code. While very similar, this is a separate issue from CVE-2022-34483. (CVE-2022-34482) - An attacker who could have convinced a user to drag and drop an image to a filesystem could have manipulated the resulting filename to contain an executable extension, and by extension potentially tricked the user into executing malicious code. While very similar, this is a separate issue from CVE-2022-34482. (CVE-2022-34483) - ASN.1 parsing of an indefinite SEQUENCE inside an indefinite GROUP could have resulted in the parser accepting malformed ASN.1. (CVE-2022-34476) - In the Less-thancodeGreater-thannsTArrayImpl::ReplaceElementsAt()Less-than/codeGreater-than function, an integer overflow could have occurred when the number of elements to replace was too large for the container. (CVE-2022-34481) - Even when an iframe was sandboxed with Less-thancodeGreater-thanallow-top-navigation-by-user-activationLess-than/codeGreater-than, if it received a redirect header to an external protocol the browser would process the redirect and prompt the user as appropriate. (CVE-2022-34474) - When a TLS Certificate error occurs on a domain protected by the HSTS header, the browser should not allow the user to bypass the certificate error. On Firefox for Android, the user was presented with the option to bypass the error; this could only have been done by the user explicitly. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2022-34469) - When downloading an update for an addon, the downloaded addon update's version was not verified to match the version selected from the manifest. If the manifest had been tampered with on the server, an attacker could trick the browser into downgrading the addon to a prior version. (CVE-2022-34471) - If there was a PAC URL set and the server that hosts the PAC was not reachable, OCSP requests would have been blocked, resulting in incorrect error pages being shown. (CVE-2022-34472) - The Less-thancodeGreater-thanms-msdtLess-than/codeGreater-than, Less-thancodeGreater-thansearchLess-than/codeGreater-than, and Less-thancodeGreater-thansearch-msLess-than/codeGreater-than protocols deliver content to Microsoft applications, bypassing the browser, when a user accepts a prompt. These applications have had known vulnerabilities, exploited in the wild (although we know of none exploited through Firefox), so in this release Firefox has blocked these protocols from prompting the user to open them. This bug only affects Firefox on Windows. Other operating systems are unaffected. (CVE-2022-34478) - If an object prototype was corrupted by an attacker, they would have been able to set undesired attributes on a JavaScript object, leading to privileged code execution. (CVE-2022-2200) - Within the Less-thancodeGreater-thanlginit()Less-than/codeGreater-than function, if several allocations succeed but then one fails, an

uninitialized pointer would have been freed despite never being allocated. (CVE-2022-34480) - The MediaError message property should be consistent to avoid leaking information about cross-origin resources; however for a same-site cross-origin resource, the message could have leaked information enabling XS-Leaks attacks. (CVE-2022-34477) - SVG Less-thancodeGreater-thanLess-thanuseGreater-thanLess-than/codeGreater-than tags that referenced a same-origin document could have resulted in script execution if attacker input was sanitized via the HTML Sanitizer API. This would have required the attacker to reference a same-origin JavaScript file containing the script to be executed. (CVE-2022-34475) - The HTML Sanitizer should have sanitized the Less-thancodeGreater-thanhrefLess-than/codeGreater-than attribute of SVG Less-thancodeGreater-thanLess-thanuseGreater-thanLess-than/codeGreater-than tags; however it incorrectly did not sanitize Less-thancodeGreater-thanxlink:hrefLess-than/codeGreater-than attributes. (CVE-2022-34473) - The Mozilla Fuzzing Team reported potential vulnerabilities present in Firefox 101 and Firefox ESR 91.10. Some of these bugs showed evidence of JavaScript prototype or memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-34484) - Mozilla developers Bryce Seager van Dyk and the Mozilla Fuzzing Team reported potential vulnerabilities present in Firefox 101. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-34485) 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 Mozilla Firefox version 102.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-24/

15. Mozilla Firefox Less-than 103.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	**Critical**	Status	**Closed**
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Closed

Description

The version of Firefox installed on the remote Windows host is prior to 103.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-28 advisory. - When combining CSS properties for overflow and transform, the mouse cursor could interact with different coordinates than

displayed. (CVE-2022-36319) - When visiting a website with an overly long URL, the user interface would start to hang. Due to session restore, this could lead to a permanent Denial of Service. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2022-36317) - When visiting directory listings for `chrome://` URLs as source text, some parameters were reflected. (CVE-2022-36318) - When opening a Windows shortcut from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This bug only affects Firefox for Windows. Other operating systems are unaffected. (CVE-2022-36314) - When loading a script with Subresource Integrity, attackers with an injection capability could trigger the reuse of previously cached entries with incorrect, different integrity metadata. (CVE-2022-36315) - When using the Performance API, an attacker was able to notice subtle differences between PerformanceEntries and thus learn whether the target URL had been subject to a redirect. (CVE-2022-36316) - Mozilla developers and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 102. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-2505, CVE-2022-36320) 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 Mozilla Firefox version 103.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-28/

16. KB5023697: Windows 10 Version 1607 and Windows Server 2016 Security Update (March 2023): The remote Windows host is affected by multiple vulnerabilities.

Severity	**Critical**	Status	**Open**
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The remote Windows host is missing security update 5023697. It is, therefore, affected by multiple vulnerabilities - An out-of-bounds write vulnerability exists in TPM2.0's Module Library allowing writing of a 2-byte data past the end of TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can lead to denial of service (crashing the TPM chip/process or rendering it unusable) and/or arbitrary code execution in the TPM context. (CVE-2023-1017) - An out-of-bounds read vulnerability exists in TPM2.0's Module Library allowing a

2-byte read past the end of a TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can read or access sensitive data stored in the TPM. (CVE-2023-1018) - Remote Procedure Call Runtime Remote Code Execution Vulnerability (CVE-2023-21708, CVE-2023-23405, CVE-2023-24869, CVE-2023-24908) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Apply Security Update 5023697
https://support.microsoft.com/help/5023697

17. KB5025230: Windows 2022 / Azure Stack HCI 22H2 Security Update (April 2023): The remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

CIT-ARCH - (10.10.50.14) - Open

CIT-MGMT - (10.10.50.25) - Open

CIT-ROOT-CA - (10.10.50.32) - Open

Description

The remote Windows host is missing security update 5025230. It is, therefore, affected by multiple vulnerabilities - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-28275) - Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability (CVE-2023-28250) - Microsoft Message Queuing Remote Code Execution Vulnerability (CVE-2023-21554) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Apply Security Update 5025230
https://support.microsoft.com/help/5025230

18. KB5025272: Windows Server 2012 Security Update (April 2023): The remote

Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

CITS8 - (10.10.50.28) - Open

Description

The remote Windows host is missing security update 5025272. It is, therefore, affected by multiple vulnerabilities - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-28275) - Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability (CVE-2023-28250) - Microsoft Message Queuing Remote Code Execution Vulnerability (CVE-2023-21554) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Apply Security Update 5025272 or Cumulative Update 5025287
https://support.microsoft.com/help/5025272 https://support.microsoft.com/help/5025287

19. KB5025228: Windows 10 Version 1607 and Windows Server 2016 Security Update (April 2023): The remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The remote Windows host is missing security update 5025228. It is, therefore, affected by multiple

vulnerabilities - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-28275) - Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability (CVE-2023-28250) - Microsoft Message Queuing Remote Code Execution Vulnerability (CVE-2023-21554) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Apply Security Update 5025228
https://support.microsoft.com/help/5025228

20. SSL Version 2 and 3 Protocol Detection: The remote service encrypts traffic using a protocol with known weaknesses.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS8 - (10.10.50.28) - Open

CIT-SQL - (10.10.50.13) - Closed

CIT-TECH - (10.40.50.97) - Closed

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.

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

21. Microsoft Edge (Chromium) Less-than 111.0.1661.54 / 110.0.1587.78 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.

Severity	**Critical**	Status	**Open**
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-MGMT - (10.10.50.25) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-ARCH - (10.10.50.14) - Closed

CITS7 - (10.10.50.27) - Closed

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 111.0.1661.54 / 110.0.1587.78. It is, therefore, affected by multiple vulnerabilities as referenced in the March 24, 2023 advisory. - Use after free in Passwords in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1528) - Out of bounds memory access in WebHID in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a malicious HID device. (Chromium security severity: High) (CVE-2023-1529) - Use after free in PDF in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1530) - Use after free in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1531) - Out of bounds read in GPU Video in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML

page. (Chromium security severity: High) (CVE-2023-1532) - Use after free in WebProtect in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1533) - Out of bounds read in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1534) 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 Microsoft Edge version 111.0.1661.54 / 110.0.1587.78 or later.

http://www.nessus.org/u?245dfb65 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1528 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1529 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1530 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1531 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1532 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1533 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1534 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28261 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28286

22. Google Chrome Less-than 112.0.5615.49 Multiple Vulnerabilities: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CIT-ARCH - (10.10.50.14) - Closed

CIT-PWS - (10.10.50.20) - Closed

CITS1 - (10.10.50.21) - Closed

cIT-RDS - (10.10.50.22) - Closed

CIT-ROOT-CA - (10.10.50.32) - Closed

NFINIT-UTIL01 - (10.10.101.101) - Closed

CIT-TECH - (10.40.50.97) - Closed

Description

The version of Google Chrome installed on the remote Windows host is prior to 112.0.5615.49. It is, therefore, affected by multiple vulnerabilities as referenced in the 2023_04_stable-channel-update-for-desktop advisory. - Heap buffer overflow in Visuals. (CVE-2023-1810) - Use after free in Frames. (CVE-2023-1811) - Out of bounds memory access in DOM Bindings. (CVE-2023-1812) - Inappropriate implementation in Extensions. (CVE-2023-1813) - Insufficient validation of untrusted input in Safe Browsing. (CVE-2023-1814) - Use after free in Networking APIs. (CVE-2023-1815) - Incorrect security UI in Picture In Picture. (CVE-2023-1816) - Insufficient policy enforcement in Intents. (CVE-2023-1817) - Use after free in Vulkan. (CVE-2023-1818) - Out of bounds read in Accessibility. (CVE-2023-1819) - Heap buffer overflow in Browser History. (CVE-2023-1820) - Inappropriate implementation in WebShare. (CVE-2023-1821) - Incorrect security UI in Navigation. (CVE-2023-1822) - Inappropriate implementation in FedCM. (CVE-2023-1823) 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 Google Chrome version 112.0.5615.49 or later.
http://www.nessus.org/u?b724610b https://crbug.com/1414018 https://crbug.com/1420510 https://crbug.com/1418224 https://crbug.com/1423258 https://crbug.com/1417325 https://crbug.com/1278708 https://crbug.com/1413919 https://crbug.com/1418061 https://crbug.com/1223346 https://crbug.com/1406588 https://crbug.com/1408120 https://crbug.com/1413618 https://crbug.com/1066555 https://crbug.com/1406900

23. KB4025339: Windows 10 Version 1607 and Windows Server 2016 July 2017 Cumulative Update: The remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS1 - (10.10.50.21) - Open

CITS4 - (10.10.50.24) - Closed

Description

The remote Windows host is missing security update KB4025339. It is, therefore, affected by multiple vulnerabilities : - An information disclosure vulnerability exists in the Windows Performance Monitor Console due to improper parsing of XML input that contains a reference to an external entity. An unauthenticated, remote attacker can exploit this, by convincing a user to create a Data Collector Set and import a specially crafted XML file, to disclose arbitrary files via an XML external entity (XXE) declaration. (CVE-2017-0170) - A remote code execution vulnerability exists in Windows Explorer due to improper handling of executable files and shares during rename operations. An unauthenticated, remote attacker can exploit this, by convincing a user to open a specially crafted file, to execute arbitrary code in the context of the current user. (CVE-2017-8463) - Multiple elevation of privilege vulnerabilities exist in the Microsoft Graphics component due to improper handling of objects in memory. A local attacker can exploit these, via a specially crafted application, to run arbitrary code in kernel mode. (CVE-2017-8467, CVE-2017-8556, CVE-2017-8573, CVE-2017-8574, CVE-2017-8577, CVE-2017-8578, CVE-2017-8580) - An information disclosure vulnerability exists in Win32k due to improper handling of objects in memory. A local attacker can exploit this, via a specially crafted application, to disclose sensitive information. (CVE-2017-8486) - A security bypass vulnerability exists in Microsoft Windows when handling Kerberos ticket exchanges due to a failure to prevent tampering with the SNAME field. A man-in-the-middle attacker can exploit this to bypass the Extended Protection for Authentication security feature. (CVE-2017-8495) - An information disclosure vulnerability exists in the Windows System Information Console due to improper parsing of XML input that contains a reference to an external entity. An unauthenticated, remote attacker can exploit this, by convincing a user to open a specially crafted file, to disclose arbitrary files via an XML external entity (XXE) declaration. (CVE-2017-8557) - An elevation of privilege vulnerability exists in the Windows kernel due to improper handling of objects in memory. A local attacker can exploit this, via a specially crafted application, to execute arbitrary code with elevated permissions. (CVE-2017-8561) - An elevation of privilege vulnerability exists in Windows due to improper handling of calls to Advanced Local Procedure Call (ALPC). An authenticated, remote attacker can exploit this via a specially crafted application, to run processes in an elevated context. (CVE-2017-8562) - An elevation of privilege vulnerability exists in Windows due to Kerberos falling back to NT LAN Manager (NTLM) Authentication Protocol as the default authentication protocol. An authenticated, remote attacker can exploit this, via an application that sends specially crafted traffic to a domain controller, to run processes in an elevated context. (CVE-2017-8563)* - An information disclosure vulnerability exists in the Windows kernel due to improper initialization of objects in memory. An authenticated, remote attacker can exploit this, via a specially crafted application, to bypass Kernel Address Space Layout Randomization (KASLR) and disclose the base address of the kernel driver. (CVE-2017-8564) - A remote code execution vulnerability exists in PowerShell when handling a PSObject that wraps a CIM instance. An authenticated, remote attacker can exploit this, via a specially crafted script, to execute arbitrary code in a PowerShell remote session. (CVE-2017-8565) - An elevation of privilege vulnerability exists in Windows Input Method Editor (IME) due to improper handling of parameters in a method of a DCOM class. A local attacker can exploit this, via a specially crafted application, to run processes in an elevated context. (CVE-2017-8566) - An elevation of privilege vulnerability exists in Windows due to improper handling of objects in memory. A local attacker can exploit this, via a

specially crafted application, to run arbitrary code in kernel mode. (CVE-2017-8581) - An information disclosure vulnerability exists in the HTTP.sys server application component due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to disclose sensitive information. (CVE-2017-8582) - A remote code execution vulnerability exists in Microsoft HoloLens due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to execute arbitrary code. (CVE-2017-8584) - A denial of service vulnerability exists in the Microsoft Common Runtime Library component due to improper handling of web requests. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to cause a denial of service condition in a .NET application. (CVE-2017-8585) - A remote code execution vulnerability exists in WordPad due to improper parsing of specially crafted files. An unauthenticated, remote attacker can exploit this, by convincing a user to open a specially crafted file, to execute arbitrary code in the context of the current user. (CVE-2017-8588) - A remote code execution vulnerability exists in the Windows Search component due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this, by sending specially crafted messages to the Windows Search service, to elevate privileges and execute arbitrary code. (CVE-2017-8589) - An elevation of privilege vulnerability exists in the Windows Common Log File System (CLFS) driver due to improper handling of objects in memory. A local attacker can exploit this, via a specially crafted application, to run processes in an elevated context. (CVE-2017-8590) - A security bypass vulnerability exists in Microsoft browsers due to improper handling of redirect requests. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to bypass CORS redirect restrictions. (CVE-2017-8592) - Multiple remote code execution vulnerability exist in Microsoft Edge in the scripting engine due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit these, by convincing a user to visit a specially crafted website, to execute arbitrary code in the context of the current user. (CVE-2017-8595, CVE-2017-8598, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8619) - A remote code execution vulnerability exists in Microsoft Edge due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to execute arbitrary code in the context of the current user. (CVE-2017-8596) - A security bypass vulnerability exists in Microsoft Edge due to a failure to correctly apply the same-origin policy for HTML elements present in other browser windows. An unauthenticated, remote attacker can exploit this, by convincing a user to follow a link, to cause the user to load a malicious website. (CVE-2017-8599) - A remote code execution vulnerability exists in Microsoft Edge in the Chakra JavaScript engine due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to execute arbitrary code in the context of the current user. (CVE-2017-8601) - A spoofing vulnerability exists in Microsoft browsers due to improper parsing of HTTP content. An unauthenticated, remote attacker can exploit this, by convincing a user to click a specially crafted URL, to redirect the user to a malicious website. (CVE-2017-8602) - Multiple remote code execution vulnerabilities exist in Microsoft browsers in the JavaScript engines due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit these, by convincing a user to visit a specially crafted website, to execute arbitrary code in the context of the current user. (CVE-2017-8606, CVE-2017-8607, CVE-2017-8608) - A remote code execution vulnerability exists in Microsoft browsers in the scripting engine due to improper handling of objects in memory. An

unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to execute arbitrary code in the context of the current user. (CVE-2017-8609) - A spoofing vulnerability exists in Microsoft Edge due to improper parsing of HTTP content. An unauthenticated, remote attacker can exploit this, by convincing a user to click a specially crafted URL, to redirect the user to a malicious website. (CVE-2017-8611) - A remote code execution vulnerability exists in Internet Explorer in the VBScript engine due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to execute arbitrary code in the context of the current user. (CVE-2017-8618) * note CVE-2017-8563 introduces a registry setting that administrators can use to help make LDAP authentication over SSL/TLS more secure, administrators need to create a LdapEnforceChannelBinding registry setting on machine running AD DS or AD LDS.

Solution

Apply security update KB4025339 as well as refer to the KB article for additional information.
http://www.nessus.org/u?9415d772 http://www.nessus.org/u?00f4a98e

24. Mozilla Firefox Less-than 109.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

LWDC-VEEAM - (10.10.50.102) - Open

CIT-TECH - (10.40.50.97) - Open

cIT-RDS - (10.10.50.22) - Closed

Description

The version of Firefox installed on the remote Windows host is prior to 109.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2023-01 advisory. - A compromised web child process could disable web security opening restrictions, leading to a new child process being spawned within the Less-thancodeGreater-thanfile://Less-than/codeGreater-than context. Given a reliable exploit primitive, this new process could be exploited again leading to arbitrary file read. (CVE-2023-23597) - Due to the Firefox GTK wrapper code's use of text/plain for drag data and GTK treating all text/plain MIMEs containing file URLs as being dragged a website could arbitrarily read a

file via a call to Less-thancodeGreater-thanDataTransfer.setDataLess-than/codeGreater-than. (CVE-2023-23598) - When copying a network request from the developer tools panel as a curl command the output was not being properly sanitized and could allow arbitrary commands to be hidden within. (CVE-2023-23599) - Per origin notification permissions were being stored in a way that didn't take into account what browsing context the permission was granted in. This lead to the possibility of notifications to be displayed during different browsing sessions. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2023-23600) - Navigations were being allowed when dragging a URL from a cross-origin iframe into the same tab which could lead to website spoofing attacks (CVE-2023-23601) - A mishandled security check when creating a WebSocket in a WebWorker caused the Content Security Policy connect-src header to be ignored. This could lead to connections to restricted origins from inside WebWorkers. (CVE-2023-23602) - Regular expressions used to filter out forbidden properties and values from style directives in calls to Less-thancodeGreater-thanconsole.logLess-than/codeGreater-than weren't accounting for external URLs. Data could then be potentially exfiltrated from the browser. (CVE-2023-23603) - A duplicate Less-thancodeGreater-thanSystemPrincipalLess-than/codeGreater-than object could be created when parsing a non-system html document via Less-thancodeGreater-thanDOMParser::ParseFromSafeStringLess-than/codeGreater-than. This could have lead to bypassing web security checks. (CVE-2023-23604) - Mozilla developers and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 108 and Firefox ESR 102.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2023-23605) - Mozilla developers and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 108. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2023-23606) 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 Mozilla Firefox version 109.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2023-01/

25. Mozilla Firefox Less-than 110.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	**Critical**	Status	**Open**
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 110.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2023-05 advisory. - The Less-thancodeGreater-thanContent-Security-Policy-Report-OnlyLess-than/codeGreater-than header could allow an attacker to leak a child iframe's unredacted URI when interaction with that iframe triggers a redirect. (CVE-2023-25728) - A background script invoking Less-thancodeGreater-thanrequestFullscreenLess-than/codeGreater-than and then blocking the main thread could force the browser into fullscreen mode indefinitely, resulting in potential user confusion or spoofing attacks. (CVE-2023-25730) - A lack of in app notification for entering fullscreen mode could have lead to a malicious website spoofing browser chrome. This bug only affects Firefox Focus. Other versions of Firefox are unaffected. (CVE-2023-25743) - An attacker could construct a PKCS 12 cert bundle in such a way that could allow for arbitrary memory writes via PKCS 12 Safe Bag attributes being mishandled. (CVE-2023-0767) - Cross-compartment wrappers wrapping a scripted proxy could have caused objects from other compartments to be stored in the main compartment resulting in a use-after-free after unwrapping the proxy. (CVE-2023-25735) - An invalid downcast from Less-thancodeGreater-thannsTextNodeLess-than/codeGreater-than to Less-thancodeGreater-thanSVGElementLess-than/codeGreater-than could have lead to undefined behavior. (CVE-2023-25737) - Members of the Less-thancodeGreater-thanDEVMODEWLess-than/codeGreater-than struct set by the printer device driver weren't being validated and could have resulted in invalid values which in turn would cause the browser to attempt out of bounds access to related variables. This bug only affects Firefox on Windows. Other operating systems are unaffected. (CVE-2023-25738) - Module load requests that failed were not being checked as to whether or not they were cancelled causing a use-after-free in Less-thancodeGreater-thanScriptLoadContextLess-than/codeGreater-than. (CVE-2023-25739) - Permission prompts for opening external schemes were only shown for Less-thancodeGreater-thanContentPrincipalsLess-than/codeGreater-than resulting in extensions being able to open them without user interaction via Less-thancodeGreater-thanExpandedPrincipalsLess-than/codeGreater-than. This could lead to further malicious actions such as downloading files or interacting with software already installed on the system. (CVE-2023-25729) - When encoding data from an Less-thancodeGreater-thaninputStreamLess-than/codeGreater-than in Less-thancodeGreater-thanxpcomLess-than/codeGreater-than the size of the input being encoded was not correctly calculated potentially leading to an out of bounds memory write. (CVE-2023-25732) - After downloading a Windows Less-thancodeGreater-than.urlLess-than/codeGreater-than shortcut from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This also had the potential to leak NTLM credentials to the resource. This bug only affects Firefox on Windows. Other operating systems are unaffected. (CVE-2023-25734) - After downloading a Windows Less-thancodeGreater-than.scfLess-

than/codeGreater-than script from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This also had the potential to leak NTLM credentials to the resource. This bug only affects Firefox for Windows. Other operating systems are unaffected. (CVE-2023-25740) - Due to URL previews in the network panel of developer tools improperly storing URLs, query parameters could potentially be used to overwrite global objects in privileged code. (CVE-2023-25731) - The return value from Less-thancodeGreater-thangfx::SourceSurfaceSkia::Map()Less-than/codeGreater-than wasn't being verified which could have potentially lead to a null pointer dereference. (CVE-2023-25733) - An invalid downcast from Less-thancodeGreater-thannsHTMLDocumentLess-than/codeGreater-than to Less-thancodeGreater-thannsIContentLess-than/codeGreater-than could have lead to undefined behavior. (CVE-2023-25736) - When dragging and dropping an image cross-origin, the image's size could potentially be leaked. This behavior was shipped in 109 and caused web compatibility problems as well as this security concern, so the behavior was disabled until further review. (CVE-2023-25741) - When importing a SPKI RSA public key as ECDSA P-256, the key would be handled incorrectly causing the tab to crash. (CVE-2023-25742) - Mozilla developers Kershaw Chang and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 109 and Firefox ESR 102.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2023-25744) - Mozilla developers Timothy Nikkel, Gabriele Svelto, Jeff Muizelaar and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 109. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2023-25745) 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 Mozilla Firefox version 110.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2023-05/

26. Mozilla Firefox Less-than 111.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	**Critical**	Status	**Open**
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 111.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2023-09 advisory. - The fullscreen notification could have been hidden on Firefox for Android by using download popups, resulting in potential user confusion or spoofing attacks. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2023-28159) - By displaying a prompt with a long description, the fullscreen notification could have been hidden, resulting in potential user confusion or spoofing attacks. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2023-25748) - Android applications with unpatched vulnerabilities can be launched from a browser using Intents, exposing users to these vulnerabilities. Firefox will now confirm with users that they want to launch an external application before doing so. This bug only affects Firefox for Android. Other versions of Firefox are unaffected. (CVE-2023-25749) - Under certain circumstances, a ServiceWorker's offline cache may have leaked to the file system when using private browsing mode. (CVE-2023-25750) - Sometimes, when invalidating JIT code while following an iterator, the newly generated code could be overwritten incorrectly. This could lead to a potentially exploitable crash. (CVE-2023-25751) - When following a redirect to a publicly accessible web extension file, the URL may have been translated to the actual local path, leaking potentially sensitive information. (CVE-2023-28160) - Dragging a URL from a cross-origin iframe that was removed during the drag could have lead to user confusion and website spoofing attacks. (CVE-2023-28164) - If temporary one-time permissions, such as the ability to use the Camera, were granted to a document loaded using a file: URL, that permission persisted in that tab for all other documents loaded from a file: URL. This is potentially dangerous if the local files came from different sources, such as in a download directory. (CVE-2023-28161) - While implementing on AudioWorklets, some code may have casted one type to another, invalid, dynamic type. This could have lead to a potentially exploitable crash. (CVE-2023-28162) - When accessing throttled streams, the count of available bytes needed to be checked in the calling function to be within bounds. This may have lead future code to be incorrect and vulnerable. (CVE-2023-25752) - When downloading files through the Save As dialog on Windows with suggested filenames containing environment variable names, Windows would have resolved those in the context of the current user. This bug only affects Firefox on Windows. Other versions of Firefox are unaffected. (CVE-2023-28163) - Mozilla developers Timothy Nikkel, Andrew McCreight, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 110 and Firefox ESR 102.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2023-28176) - Mozilla developers and community members Calixte Denizet, Gabriele Svelto, Andrew McCreight, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 110. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2023-28177) 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 Mozilla Firefox version 111.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2023-09/

27. JBoss Enterprise Application Platform doFilter() Method Insecure Deserialization RCE: The remote host is affected by a remote code execution vulnerability.

Severity	Critical	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CITS7 - WAN - (70.167.3.27) - Open

CITS7 - (10.10.50.27) - Closed

Description

The JBoss Application Server installed on the remote host is affected by a remote code execution vulnerability. A flaw in the doFilter method of the ReadOnlyAccessFilter class, of the HTTP Invoker service doesn't restrict classes for which it performs deserialization. This allows a remote, unauthenticated attacker to execute arbitrary code via crafted serialized data. To conduct more accurate test and get precise evidence of RCE exploitation please set 'Perform thorough tests (may disrupt your network or impact scan speed)' setting in the Scan Configuration.

Solution

Follow mitigation guidelines provided in the Red Hat Advisory for CVE-2017-12149.
https://access.redhat.com/security/cve/cve-2017-12149

28. KB5022895: Windows Server 2012 Security Update (February 2023): The remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS8 - (10.10.50.28) - Open

Description

The remote Windows host is missing security update 5022895. It is, therefore, affected by multiple vulnerabilities - Microsoft PostScript Printer Driver Remote Code Execution Vulnerability (CVE-2023-21684, CVE-2023-21801) - Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2023-21685, CVE-2023-21686, CVE-2023-21799) - Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability (CVE-2023-21689) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Apply Security Update 5022895 or Cumulative Update 5022903
https://support.microsoft.com/help/5022895 https://support.microsoft.com/help/5022903

29. KB5023752: Windows Server 2012 Security Update (March 2023): The remote Windows host is affected by multiple vulnerabilities.

Severity	**Critical**	Status	**Open**
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS8 - (10.10.50.28) - Open

Description

The remote Windows host is missing security update 5023752. It is, therefore, affected by multiple vulnerabilities - Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability (CVE-2023-23415) - Remote Procedure Call Runtime Remote Code Execution Vulnerability (CVE-2023-21708, CVE-2023-23405, CVE-2023-24869, CVE-2023-24908) - Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability (CVE-2023-23385) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Apply Security Update 5023752 or Cumulative Update 5023756
https://support.microsoft.com/help/5023752 https://support.microsoft.com/help/5023756

30. Apache Log4j 1.x Multiple Vulnerabilities: A logging library running on the remote host has multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-FS - (10.10.50.30) - Open

CIT-TECH - (10.40.50.97) - Open

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.
https://logging.apache.org/log4j/1.2/

31. Oracle Java SE 1.7.0_241 / 1.8.0_231 / 1.11.0_5 / 1.13.0_1 Multiple Vulnerabilities (Oct 2019 CPU) (Windows): The remote Windows host contains a programming platform that is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 241, 8 Update 231, 11 Update 5, or 13 Update 1. It is, therefore, affected by multiple vulnerabilities related to the following components : - 2D - Libraries - Kerberos - Networking - JavaFX - Hotspot - Scripting - Javadoc - Deployment - Concurrency - JAXP - Serialization - Security Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Oracle JDK / JRE 13 Update 1, 11 Update 5, 8 Update 231 / 7 Update 241 or later. If necessary, remove any affected versions.
http://www.nessus.org/u?2c94f8e4 http://www.nessus.org/u?144b1a0e

32. Mozilla Firefox Less-than 107.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

LWDC-VEEAM - (10.10.50.102) - Open

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 107.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-47 advisory. - Service Workers should not be able to infer information about opaque cross-origin responses; but timing information for cross-origin media combined with Range requests might have allowed them to determine the presence or length of a media file. (CVE-2022-45403) - Through a series of popup and Less-thancodeGreater-thanwindow.print()Less-than/codeGreater-than calls, an attacker can cause a window to go fullscreen without the user seeing the notification prompt, resulting in potential user confusion or spoofing attacks. (CVE-2022-45404) - Freeing arbitrary Less-thancodeGreater-thannsIInputStreamLess-than/codeGreater-than's on a different thread than creation could have led to a use-after-free and potentially exploitable crash. (CVE-2022-45405) - If an out-of-memory condition occurred when creating a JavaScript global, a JavaScript realm may be deleted while references to it lived on in a BaseShape. This could lead to a use-after-free causing a potentially exploitable crash. (CVE-2022-45406) - If an attacker loaded a font using Less-thancodeGreater-thanFontFace()Less-than/codeGreater-than on a background worker, a use-after-free could have occurred, leading to a potentially exploitable crash. (CVE-2022-45407) - Through a series of popups that reuse windowName, an attacker can cause a window to go fullscreen without the user seeing the notification prompt, resulting in potential user confusion or spoofing attacks. (CVE-2022-45408) - The garbage collector could have been aborted in several states and zones and Less-thancodeGreater-thanGCRuntime::finishCollectionLess-than/codeGreater-than may not have been called, leading to a use-after-free and potentially exploitable crash (CVE-2022-45409) - When a ServiceWorker intercepted a request with Less-thancodeGreater-thanFetchEventLess-than/codeGreater-than, the origin of the request was lost after the ServiceWorker took ownership of it. This had the effect of negating SameSite cookie protections. This was addressed in the spec and then in browsers. (CVE-2022-45410) - Cross-Site Tracing occurs when a server will echo a request back via the Trace method, allowing an XSS attack to access to authorization headers and cookies inaccessible to JavaScript (such as cookies protected by HTTPOnly). To mitigate this attack, browsers placed limits on Less-thancodeGreater-thanfetch()Less-than/codeGreater-than and XMLHttpRequest; however some webservers have implemented non-standard headers such as Less-thancodeGreater-thanX-Http-Method- OverrideLess-than/codeGreater-than that override the HTTP method, and made this attack possible again. Firefox has applied the same mitigations to the use of this and similar headers. (CVE-2022-45411) - When resolving a symlink such as Less-thancodeGreater-thanfile:///proc/self/fd/1Less-than/codeGreater-than, an error message may be produced where the symlink was resolved to a string containing unitialized memory in the buffer. This bug only affects Firefox on Unix-based operated systems (Android, Linux, MacOS). Windows is unaffected. (CVE-2022-45412) - Using the Less-thancodeGreater-thanS.browserfallbackurl parameterLess-than/codeGreater-than parameter, an attacker could redirect a user to a URL and cause SameSite=Strict cookies to be sent. This issue only affects Firefox for Android. Other operating systems are not affected. (CVE-2022-45413) - A flaw in XML parsing could have led to a use-after-free causing a potentially exploitable crash. In official releases of Firefox this vulnerability is mitigated

by wasm sandboxing; versions managed by Linux distributions may have other settings. (CVE-2022-40674) - When downloading an HTML file, if the title of the page was formatted as a filename with a malicious extension, Firefox may have saved the file with that extension, leading to possible system compromise if the downloaded file was later ran. (CVE-2022-45415) - Keyboard events reference strings like KeyA that were at fixed, known, and widely-spread addresses. Cache-based timing attacks such as Prime+Probe could have possibly figured out which keys were being pressed. (CVE-2022-45416) - Service Workers did not detect Private Browsing Mode correctly in all cases, which could have led to Service Workers being written to disk for websites visited in Private Browsing Mode. This would not have persisted them in a state where they would run again, but it would have leaked Private Browsing Mode details to disk. (CVE-2022-45417) - If a custom mouse cursor is specified in CSS, under certain circumstances the cursor could have been drawn over the browser UI, resulting in potential user confusion or spoofing attacks. (CVE-2022-45418) - If the user added a security exception for an invalid TLS certificate, opened an ongoing TLS connection with a server that used that certificate, and then deleted the exception, Firefox would have kept the connection alive, making it seem like the certificate was still trusted. (CVE-2022-45419) - Using tables inside of an iframe, an attacker could have caused iframe contents to be rendered outside the boundaries of the iframe, resulting in potential user confusion or spoofing attacks. (CVE-2022-45420) - Mozilla developers Andrew McCreight and Gabriele Svelto reported memory safety bugs present in Firefox 106 and Firefox ESR 102.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-45421) 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 Mozilla Firefox version 107.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-47/

33. Microsoft Silverlight Unsupported Version Detection (Windows): The remote host has an unsupported version of Microsoft Silverlight.

Severity	**Critical**	Status	**Open**
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The installation of Microsoft Silverlight on the Windows 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

Remove Microsoft Silverlight.
http://www.nessus.org/u?fcc00b67

34. PuTTY Less-than 0.71 Multiple Vulnerabilities: The remote Windows host has an SSH client that is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The remote host has a version of PuTTY installed that is prior to 0.71. It is, therefore, affected by multiple vulnerabilities including: - A remotely triggerable buffer overflow in any kind of server-to-client forwarding. (CVE-2019-9895) - Potential recycling of random numbers used in cryptography. (CVE-2019-9898) - A remotely triggerable memory overwrite in RSA key exchange can occur before host key verification. (CVE-2019-9894)

Solution

Upgrade to PuTTY version 0.71 or later.
http://www.nessus.org/u?fc188a9c http://www.nessus.org/u?cd82820f
http://www.nessus.org/u?e116cf63 http://www.nessus.org/u?39988fba
http://www.nessus.org/u?50d03d73 http://www.nessus.org/u?dc4b5e69
http://www.nessus.org/u?d52aebfd http://www.nessus.org/u?819250a8
http://www.chiark.greenend.org.uk/~sgtatham/putty/changes.html

35. Mozilla Firefox Less-than 90.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 90.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-28 advisory. - A malicious webpage could have triggered a use-after-free, memory corruption, and a potentially exploitable crash. This bug only affected Firefox when accessibility was enabled. (CVE-2021-29970) - If a user had granted a permission to a webpage and saved that grant, any webpage running on the same host - irrespective of scheme or port - would be granted that permission.This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29971) - An out of bounds write in ANGLE could have allowed an attacker to corrupt memory leading to a potentially exploitable crash. (CVE-2021-30547) - A user-after-free vulnerability was found via testing, and traced to an out-of-date Cairo library. Updating the library resolved the issue, and may have remediated other, unknown security vulnerabilities as well. (CVE-2021-29972) - Password autofill was enabled without user interaction on insecure websites on Firefox for Android. This was corrected to require user interaction with the page before a user's password would be entered by the browser's autofill functionality.This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29973) - When network partitioning was enabled, e.g. as a result of Enhanced Tracking Protection settings, a TLS error page would allow the user to override an error on a domain which had specified HTTP Strict Transport Security (which implies that the error should not be override-able.) This issue did not affect the network connections, and they were correctly upgraded to HTTPS automatically. (CVE-2021-29974) - Through a series of DOM manipulations, a message, over which the attacker had control of the text but not HTML or formatting, could be overlaid on top of another domain (with the new domain correctly shown in the address bar) resulting in possible user confusion. (CVE-2021-29975) - Mozilla developers Emil Ghitta, Tyson Smith, Valentin Gosu, Olli Pettay, and Randell Jesup reported memory safety bugs present in Firefox 89 and Firefox ESR 78.11. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29976) - Mozilla developers Andrew McCreight, Tyson Smith, Christian Holler, and Gabriele Svelto reported memory safety bugs present in Firefox 89. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29977) 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 Mozilla Firefox version 90.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2021-28/

36. Mozilla Firefox Less-than 97.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 97.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-04 advisory. - A Time-of-Check Time-of-Use bug existed in the Maintenance (Updater) Service that could be abused to grant Users write access to an arbitrary directory. This could have been used to escalate to SYSTEM access. This bug only affects Firefox on Windows. Other operating systems are unaffected. (CVE-2022-22753) - If a user installed an extension of a particular type, the extension could have auto-updated itself and while doing so, bypass the prompt which grants the new version the new requested permissions. (CVE-2022-22754) - By using XSL Transforms, a malicious webserver could have served a user an XSL document that would continue to execute JavaScript (within the bounds of the same-origin policy) even after the tab was closed. (CVE-2022-22755) - If a user was convinced to drag and drop an image to their desktop or other folder, the resulting object could have been changed into an executable script which would have run arbitrary code after the user clicked on it. (CVE-2022-22756) - Remote Agent, used in WebDriver, did not validate the Host or Origin headers. This could have allowed websites to connect back locally to the user's browser to control it. This bug only affected Firefox when WebDriver was enabled, which is not the default configuration. (CVE-2022-22757) - When clicking on a tel: link, USSD codes, specified after a Less-thancodeGreater-thanLess-than/codeGreater-than character, would be included in the phone number. On certain phones, or on certain carriers, if the number was dialed this could perform actions on a user's account, similar to a cross-site request forgery attack. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2022-22758) - If a document created a sandboxed iframe without Less-thancodeGreater-thanallow-scriptsLess-than/codeGreater-than, and subsequently appended an element to the iframe's document that e.g. had a JavaScript event handler - the event handler would have run despite the iframe's sandbox. (CVE-2022-22759) - When importing resources using Web Workers, error messages would distinguish the difference between Less-thancodeGreater-

thanapplication/javascriptLess-than/codeGreater-than responses and non-script responses. This could have been abused to learn information cross-origin. (CVE-2022-22760) - Web-accessible extension pages (pages with a moz-extension:// scheme) were not correctly enforcing the frame-ancestors directive when it was used in the Web Extension's Content Security Policy. (CVE-2022-22761) - Under certain circumstances, a JavaScript alert (or prompt) could have been shown while another website was displayed underneath it. This could have been abused to trick the user. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2022-22762) - Mozilla developers Paul Adenot and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 96 and Firefox ESR 91.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-22764) - Mozilla developers and community members Gabriele Svelto, Sebastian Hengst, Randell Jesup, Luan Herrera, Lars T Hansen, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 96. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-0511) 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 Mozilla Firefox version 97.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-04/

37. Mozilla Firefox Less-than 97.0.2: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 97.0.2. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-09 advisory. - Removing an XSLT parameter during processing could have lead to an exploitable use-after-free. We have had reports of attacks in the wild abusing this flaw. (CVE-2022-26485) - An unexpected message in the WebGPU IPC framework could lead to a use-after-free and exploitable sandbox escape. We have had reports of attacks in the wild abusing this flaw. (CVE-2022-26486) 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 Mozilla Firefox version 97.0.2 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/

38. Mozilla Firefox Less-than 98.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	Critical	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 98.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-10 advisory. - When resizing a popup after requesting fullscreen access, the popup would not display the fullscreen notification. (CVE-2022-26383) - If an attacker could control the contents of an iframe sandboxed with Less-thancodeGreater-thanallow-popupsLess-than/codeGreater-than but not Less-thancodeGreater-thanallow-scriptsLess-than/codeGreater-than, they were able to craft a link that, when clicked, would lead to JavaScript execution in violation of the sandbox. (CVE-2022-26384) - When installing an add-on, Firefox verified the signature before prompting the user; but while the user was confirming the prompt, the underlying add-on file could have been modified and Firefox would not have noticed. (CVE-2022-26387) - An attacker could have caused a use-after-free by forcing a text reflow in an SVG object leading to a potentially exploitable crash. (CVE-2022-26381) - While the text displayed in Autofill tooltips cannot be directly read by JavaScript, the text was rendered using page fonts. Side-channel attacks on the text by using specially crafted fonts could have lead to this text being inferred by the webpage. (CVE-2022-26382) - In unusual circumstances, an individual thread may outlive the thread's manager during shutdown. This could have led to a use-after-free causing a potentially exploitable crash. (CVE-2022-26385) - Mozilla developers Kershaw Chang, Ryan VanderMeulen, and Randell Jesup reported memory safety bugs present in Firefox 97. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-0843) 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 Mozilla Firefox version 98.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-10/

39. Foxit PDF Reader Less-than 12.1.2 Multiple Vulnerabilities: A PDF viewer installed on the remote Windows host is affected by multiple vulnerabilities

Severity	Critical	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

CIT-ARCH - (10.10.50.14) - Open

Description

According to its version, the Foxit PDF Reader application (previously named Foxit Reader) installed on the remote Windows host is prior to 12.1.2. It is, therefore affected by multiple vulnerabilities: 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 Foxit PDF Reader version 12.1.2 or later
http://www.nessus.org/u?a27a3e57

40. Oracle Java SE 1.7.0_221 / 1.8.0_211 / 1.11.0_3 / 1.12.0_1 Multiple Vulnerabilities (Apr 2019 CPU): The remote Windows host contains a programming platform that is affected by multiple vulnerabilities.

Severity	Critical	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

LWDC-VEEAM - (10.10.50.102) - Closed

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 221, 8 Update 211, 11 Update 3, or 12 Update 1. It is, therefore, affected by multiple vulnerabilities related to the following components : - 2D - Libraries - RMI - Windows DLL Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Oracle JDK / JRE 12 Update 1 , 11 Update 3, 8 Update 211 / 7 Update 221 or later. If necessary, remove any affected versions.
http://www.nessus.org/u?9166970d http://www.nessus.org/u?aa0c1228

41. Security Updates for Microsoft .NET core (March 2022): The Microsoft .NET core installations on the remote host are affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The Microsoft .NET core installations on the remote host are missing security updates. It is, therefore, affected by multiple vulnerabilities: - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2022-24464) - A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2020-8927, CVE-2022-24512) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update .NET Core Runtime to version 3.1.23, 5.0.15 or 6.0.3.
https://dotnet.microsoft.com/download/dotnet/3.1 https://dotnet.microsoft.com/download/dotnet/5.0

https://dotnet.microsoft.com/download/dotnet/6.0
https://github.com/dotnet/announcements/issues/210 http://www.nessus.org/u?56caba70
http://www.nessus.org/u?95177a8e http://www.nessus.org/u?96c2a71d

42. Mozilla Firefox Less-than 99.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 99.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-13 advisory. - Less-thancodeGreater-thanNSSTokenLess-than/codeGreater-than objects were referenced via direct points, and could have been accessed in an unsafe way on different threads, leading to a use-after-free and potentially exploitable crash. (CVE-2022-1097) - If a compromised content process sent an unexpected number of WebAuthN Extensions in a Register command to the parent process, an out of bounds write would have occurred leading to memory corruption and a potentially exploitable crash. (CVE-2022-28281) - By using a link with Less-thancodeGreater-thanrel=localizationLess-than/codeGreater-than a use-after-free could have been triggered by destroying an object during JavaScript execution and then referencing the object through a freed pointer, leading to a potentially exploitable crash. (CVE-2022-28282) - The sourceMapURL feature in devtools was missing security checks that would have allowed a webpage to attempt to include local files or other files that should have been inaccessible. (CVE-2022-28283) - SVG's Less-thancodeGreater-thanLess-thanuseGreater-thanLess-than/codeGreater-than element could have been used to load unexpected content that could have executed script in certain circumstances. While the specification seems to allow this, other browsers do not, and web developers relied on this property for script security so gecko's implementation was aligned with theirs. (CVE-2022-28284) - When generating the assembly code for Less-thancodeGreater-thanMLoadTypedArrayElementHoleLess-than/codeGreater-than, an incorrect AliasSet was used. In conjunction with another vulnerability this could have been used for an out of bounds memory read. (CVE-2022-28285) - Due to a layout change, iframe contents could have been rendered outside of its border. This could have led to user confusion or spoofing attacks. (CVE-2022-28286) - In unusual circumstances, selecting text could cause text selection caching to behave incorrectly, leading to a crash. (CVE-2022-28287) - The rust regex crate did not properly

prevent crafted regular expressions from taking an arbitrary amount of time during parsing. If an attacker was able to supply input to this crate, they could have caused a denial of service in the browser. (CVE-2022-24713) - Mozilla developers and community members Nika Layzell, Andrew McCreight, Gabriele Svelto, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 98 and Firefox ESR 91.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-28289) - Mozilla developers and community members Randell Jesup, Sebastian Hengst, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 98. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-28288) 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 Mozilla Firefox version 99.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-13/

43. Mozilla Firefox Less-than 100.0.2: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 100.0.2. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-19 advisory. - If an attacker was able to corrupt the methods of an Array object in JavaScript via prototype pollution, they could have achieved execution of attacker-controlled JavaScript code in a privileged context. (CVE-2022-1802) - An attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process. (CVE-2022-1529) 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 Mozilla Firefox version 100.0.2 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/

44. Mozilla Firefox Less-than 104.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 104.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-33 advisory. - An attacker could have abused XSLT error handling to associate attacker-controlled content with another origin which was displayed in the address bar. This could have been used to fool the user into submitting data intended for the spoofed origin. (CVE-2022-38472) - A cross-origin iframe referencing an XSLT document would inherit the parent domain's permissions (such as microphone or camera access). (CVE-2022-38473) - A website that had permission to access the microphone could record audio without the audio notification being shown. This bug does not allow the attacker to bypass the permission prompt - it only affects the notification shown once permission has been granted.Less-thanbr /Greater-thanThis bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2022-38474) - An attacker could have written a value to the first element in a zero-length JavaScript array. Although the array was zero-length, the value was not written to an invalid memory address. (CVE-2022-38475) - Mozilla developer Nika Layzell and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 103 and Firefox ESR 102.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-38477) - Members the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 103, Firefox ESR 102.1, and Firefox ESR 91.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-38478) 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 Mozilla Firefox version 104.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-33/

45. Mozilla Firefox Less-than 105.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 105.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-40 advisory. - During iframe navigation, certain pages did not have their FeaturePolicy fully initialized leading to a bypass that leaked device permissions into untrusted subdocuments. (CVE-2022-40959) - Concurrent use of the URL parser with non-UTF-8 data was not thread-safe. This could lead to a use-after- free causing a potentially exploitable crash. (CVE-2022-40960) - By injecting a cookie with certain special characters, an attacker on a shared subdomain which is not a secure context could set and thus overwrite cookies from a secure context, leading to session fixation and other attacks. (CVE-2022-40958) - During startup, a graphics driver with an unexpected name could lead to a stack-buffer overflow causing a potentially exploitable crash. This issue only affects Firefox for Android. Other operating systems are not affected. (CVE-2022-40961) - When injecting an HTML base element, some requests would ignore the CSP's base-uri settings and accept the injected element's base instead. (CVE-2022-40956) - Inconsistent data in instruction and data cache when creating wasm code could lead to a potentially exploitable crash. This bug only affects Firefox on ARM64 platforms. (CVE-2022-40957) - Mozilla developers Nika Layzell, Timothy Nikkel, Jeff Muizelaar, Sebastian Hengst, Andreas Pehrson, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 104 and Firefox ESR 102.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-40962) 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 Mozilla Firefox version 105.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-40/

46. Mozilla Firefox Less-than 106.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 106.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-44 advisory. - A same-origin policy violation could have allowed the theft of cross-origin URL entries, leaking the result of a redirect, via Less-thancodeGreater-thanperformance.getEntries()Less-than/codeGreater-than. (CVE-2022-42927) - Certain types of allocations were missing annotations that, if the Garbage Collector was in a specific state, could have lead to memory corruption and a potentially exploitable crash. (CVE-2022-42928) - If a website called Less-thancodeGreater-thanwindow.print()Less-than/codeGreater-than in a particular way, it could cause a denial of service of the browser, which may persist beyond browser restart depending on the user's session restore settings. (CVE-2022-42929) - If two Workers were simultaneously initializing their CacheStorage, a data race could have occurred in the Less-thancodeGreater-thanThirdPartyUtilLess-than/codeGreater-than component. (CVE-2022-42930) - Logins saved by Firefox should be managed by the Password Manager component which uses encryption to save files on-disk. Instead, the username (not password) was saved by the Form Manager to an unencrypted file on disk. (CVE-2022-42931) - Mozilla developers Ashley Hale and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 105 and Firefox ESR 102.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-42932) 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 Mozilla Firefox version 106.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-44/

47. Security Updates for Microsoft .NET Core (December 2022): The Microsoft .NET core installations on the remote host are affected by remote code execution vulnerability.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

A remote code execution vulnerability exists in .NET Core 3.1, .NET 6.0, and .NET 7.0, where a malicious actor could cause a user to run arbitrary code as a result of parsing maliciously crafted xps files. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update .NET Core Runtime to version 3.1.32 or 6.0.12 or 7.0.1.
https://support.microsoft.com/en-us/help/5021953 https://support.microsoft.com/en-us/help/5021954 https://support.microsoft.com/en-us/help/5021955

48. Security Updates for Microsoft ASP.NET Core (December 2022): The Microsoft ASP.NET core installations on the remote host are affected by remote code execution vulnerability.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

A remote code execution vulnerability exists in ASP.NET core 3.1, ASP.NET 6.0, and ASP.NET 7.0, where a malicious actor could cause a user to run arbitrary code as a result of parsing maliciously crafted xps files. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update ASP.NET Core Runtime to version 3.1.32 or 6.0.12 or 7.0.1.
https://support.microsoft.com/en-us/help/5021953 https://support.microsoft.com/en-us/help/5021954 https://support.microsoft.com/en-us/help/5021955

49. Microsoft Edge (Chromium) Less-than 112.0.1722.48 : The remote host has an web browser installed that is affected by a vulnerability.

Severity	High	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

CIT-ARCH - (10.10.50.14) - Open

CIT-MGMT - (10.10.50.25) - Open

CITS7 - (10.10.50.27) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 112.0.1722.48. It is, therefore, affected by a vulnerability as referenced in the April 15, 2023 advisory. - Type confusion in V8 in Google Chrome prior to 112.0.5615.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-2033) 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 Microsoft Edge version 112.0.1722.48 or later.
http://www.nessus.org/u?245dfb65 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2033

50. Microsoft Edge (Chromium) Less-than 112.0.1722.58 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

CIT-ARCH - (10.10.50.14) - Open

CIT-MGMT - (10.10.50.25) - Open

CITS7 - (10.10.50.27) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 112.0.1722.58. It is, therefore, affected by multiple vulnerabilities as referenced in the April 21, 2023 advisory. - Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-2133, CVE-2023-2134) - Use after free in DevTools in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who convinced a user to enable specific preconditions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-2135) - Heap buffer overflow in sqlite in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-2137) 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 Microsoft Edge version 112.0.1722.58 or later.
http://www.nessus.org/u?245dfb65 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2133 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2134 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2135 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2137

51. Microsoft Edge (Chromium) Less-than 111.0.1661.41 / 110.0.1587.69 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-ARCH - (10.10.50.14) - Open

CIT-MGMT - (10.10.50.25) - Open

CITS7 - (10.10.50.27) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 111.0.1661.41 / 110.0.1587.69. It is, therefore, affected by multiple vulnerabilities as referenced in the March 13, 2023 advisory. - Use after free in Swiftshader in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1213) - Type confusion in V8 in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1214) - Type confusion in CSS in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1215) - Use after free in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had convienced the user to engage in direct UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1216) - Stack buffer overflow in Crash reporting in Google Chrome on Windows prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1217) - Use after free in WebRTC in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1218) - Heap buffer overflow in Metrics in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1219) - Heap buffer overflow in UMA in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1220) - Insufficient policy enforcement in Extensions API in Google Chrome prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium) (CVE-2023-1221) - Heap buffer

overflow in Web Audio API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-1222) - Insufficient policy enforcement in Autofill in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-1223) - Insufficient policy enforcement in Web Payments API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-1224) - Insufficient policy enforcement in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-1228) - Inappropriate implementation in Permission prompts in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-1229) - Inappropriate implementation in WebApp Installs in Google Chrome on Android prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious WebApp to spoof the contents of the PWA installer via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-1230) - Inappropriate implementation in Autofill in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to potentially spoof the contents of the omnibox via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-1231) - Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to obtain potentially sensitive information from API via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-1232) - Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from API via a crafted Chrome Extension. (Chromium security severity: Low) (CVE-2023-1233) - Inappropriate implementation in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-1234) - Type confusion in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted UI interaction. (Chromium security severity: Low) (CVE-2023-1235) - Inappropriate implementation in Internals in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to spoof the origin of an iframe via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-1236) 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 Microsoft Edge version 111.0.1661.41 / 110.0.1587.69 or later.

http://www.nessus.org/u?245dfb65 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1213 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1214 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1215 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1216 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1217 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1218 https://msrc.microsoft.com/update-

guide/vulnerability/CVE-2023-1219 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1220 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1221 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1222 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1223 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1224 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1228 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1229 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1230 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1231 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1232 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1233 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1234 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1235 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-1236

52. Microsoft Edge (Chromium) Less-than 110.0.1587.41 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS7 - (10.10.50.27) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 110.0.1587.41. It is, therefore, affected by multiple vulnerabilities as referenced in the February 9, 2023 advisory. - Type confusion in V8 in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0696) - Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 110.0.5481.77 allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0697) - Out of bounds read in WebRTC in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0698) - Use

after free in GPU in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page and browser shutdown. (Chromium security severity: Medium) (CVE-2023-0699) - Inappropriate implementation in Download in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-0700) - Heap buffer overflow in WebUI in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via UI interaction . (Chromium security severity: Medium) (CVE-2023-0701) - Type confusion in Data Transfer in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-0702) - Type confusion in DevTools in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via UI interactions. (Chromium security severity: Medium) (CVE-2023-0703) - Insufficient policy enforcement in DevTools in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to bypass same origin policy and proxy settings via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-0704) - Integer overflow in Core in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who had one a race condition to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-0705) 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 Microsoft Edge version 110.0.1587.41 or later.

http://www.nessus.org/u?245dfb65 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0696 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0697 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0698 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0699 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0700 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0701 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0702 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0703 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0704 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0705 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21794

53. Microsoft Edge (Chromium) Less-than 110.0.1587.56 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.

Severity	High	Status	Open

First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS7 - (10.10.50.27) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 110.0.1587.56. It is, therefore, affected by multiple vulnerabilities as referenced in the February 25, 2023 advisory. - Use after free in Web Payments API in Google Chrome on Android prior to 110.0.5481.177 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0927) - Use after free in SwiftShader in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0928) - Use after free in Vulkan in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0929) - Heap buffer overflow in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0930) - Use after free in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0931) - Use after free in WebRTC in Google Chrome on Windows prior to 110.0.5481.177 allowed a remote attacker who convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0932) - Integer overflow in PDF in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium) (CVE-2023-0933) - Use after free in Prompts in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) (CVE-2023-0941) 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 Microsoft Edge version 110.0.1587.56 or later.

http://www.nessus.org/u?245dfb65 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0927 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0928 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0929 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0930 https://msrc.microsoft.com/update-

guide/vulnerability/CVE-2023-0931 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-0932 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-0933 https://msrc.microsoft.com/update-
guide/vulnerability/CVE-2023-0941

54. Security Updates for Microsoft SQL Server (February 2023): The Microsoft SQL Server installation on the remote host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS8 - (10.10.50.28) - Open

Description

The Microsoft SQL Server installation on the remote host is missing security updates. 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-2023-21528, CVE-2023-21568, CVE-2023-21704, CVE-2023-21705, CVE-2023-21713, CVE-2023-21718)

Solution

Microsoft has released the following security updates to address this issue: -KB5021126 -KB5021129 -KB5021522 -KB5021127 -KB5021045 -KB5021037 -KB5021128 -KB5021124 -KB5021125 -KB5020863 -KB5021112 -KB5021123

https://support.microsoft.com/en-us/help/5020863 https://support.microsoft.com/en-us/help/5021112
https://support.microsoft.com/en-us/help/5021126 https://support.microsoft.com/en-us/help/5021129
https://support.microsoft.com/en-us/help/5021522 https://support.microsoft.com/en-us/help/5021127
https://support.microsoft.com/en-us/help/5021045 https://support.microsoft.com/en-us/help/5021037
https://support.microsoft.com/en-us/help/5021128 https://support.microsoft.com/en-us/help/5021123
https://support.microsoft.com/en-us/help/5021124 https://support.microsoft.com/en-us/help/5021125

55. Mozilla Firefox Less-than 108.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	High	Status	Open

First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

LWDC-VEEAM - (10.10.50.102) - Open

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 108.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-51 advisory. - An out of date library (libusrsctp) contained vulnerabilities that could potentially be exploited. (CVE-2022-46871) - An attacker who compromised a content process could have partially escaped the sandbox to read arbitrary files via clipboard-related IPC messages. This bug only affects Firefox for Linux. Other operating systems are unaffected. (CVE-2022-46872) - Because Firefox did not implement the Less-thancodeGreater-thanunsafe-hashesLess-than/codeGreater-than CSP directive, an attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able to inject executable script. This would be severely constrained by the specified Content Security Policy of the document. (CVE-2022-46873) - A file with a long filename could have had its filename truncated to remove the valid extension, leaving a malicious extension in its place. This could have potentially led to user confusion and the execution of malicious code. (CVE-2022-46874) - The executable file warning was not presented when downloading .atloc and .ftploc files, which can run commands on a user's computer. Note: This issue only affected Mac OS operating systems. Other operating systems are unaffected. (CVE-2022-46875) - By confusing the browser, the fullscreen notification could have been delayed or suppressed, resulting in potential user confusion or spoofing attacks. (CVE-2022-46877) - Mozilla developers Randell Jesup, Valentin Gosu, Olli Pettay, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 107 and Firefox ESR 102.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-46878) - Mozilla developers and community members Lukas Bernhard, Gabriele Svelto, Randell Jesup, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 107. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-46879) 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 Mozilla Firefox version 108.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2022-51/

56. Mozilla Firefox Less-than 89.0: A web browser installed on the remote Windows host

is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 89.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-23 advisory. - A malicious website that causes an HTTP Authentication dialog to be spawned could trick the built-in password manager to suggest passwords for the currently active website instead of the website that triggered the dialog. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29965) - Firefox used to cache the last filename used for printing a file. When generating a filename for printing, Firefox usually suggests the web page title. The caching and suggestion techniques combined may have lead to the title of a website visited during private browsing mode being stored on disk. (CVE-2021-29960) - When styling and rendering an oversized `` element, Firefox did not apply correct clipping which allowed an attacker to paint over the user interface. (CVE-2021-29961) - Address bar search suggestions in private browsing mode were re-using session data from normal mode. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29963) - A locally-installed hostile program could send `WMCOPYDATA` messages that Firefox would process incorrectly, leading to an out-of-bounds read. This bug only affects Firefox on Windows. Other operating systems are unaffected. (CVE-2021-29964) - When a user has already allowed a website to access microphone and camera, disabling camera sharing would not fully prevent the website from re-enabling it without an additional prompt. This was only possible if the website kept recording with the microphone until re-enabling the camera. (CVE-2021-29959) - Firefox for Android would become unstable and hard-to-recover when a website opened too many popups. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29962) - Mozilla developers Christian Holler, Anny Gakhokidze, Alexandru Michis, Gabriele Svelto reported memory safety bugs present in Firefox 88 and Firefox ESR 78.11. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29967) - Mozilla developers Christian Holler, Tooru Fujisawa, Tyson Smith reported memory safety bugs present in Firefox 88. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29966) 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 Mozilla Firefox version 89.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2021-23/

57. Mozilla Firefox Less-than 91.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 91.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-33 advisory. - A suspected race condition when calling getaddrinfo led to memory corruption and a potentially exploitable crash. Note: This issue only affected Linux operating systems. Other operating systems are unaffected. (CVE-2021-29986) - An issue present in lowering/register allocation could have led to obscure but deterministic register confusion failures in JITted code that would lead to a potentially exploitable crash. (CVE-2021-29981) - Firefox incorrectly treated an inline list-item element as a block element, resulting in an out of bounds read or memory corruption, and a potentially exploitable crash. (CVE-2021-29988) - Firefox for Android could get stuck in fullscreen mode and not exit it even after normal interactions that should cause it to exit. Note: This issue only affected Firefox for Android. Other operating systems are unaffected. (CVE-2021-29983) - Instruction reordering resulted in a sequence of instructions that would cause an object to be incorrectly considered during garbage collection. This led to memory corruption and a potentially exploitable crash. (CVE-2021-29984) - Uninitialized memory in a canvas object could have caused an incorrect free() leading to memory corruption and a potentially exploitable crash. (CVE-2021-29980) - After requesting multiple permissions, and closing the first permission panel, subsequent permission panels will be displayed in a different position but still record a click in the default location, making it possible to trick a user into accepting a permission they did not want to.This bug only affects Firefox on Linux. Other operating systems are unaffected. (CVE-2021-29987) - A use-after-free vulnerability in media channels could have led to memory corruption and a potentially exploitable crash. (CVE-2021-29985) - Due to incorrect JIT optimization, we incorrectly interpreted data from the wrong type of object, resulting in the potential leak of a single bit of memory. (CVE-2021-29982) - Mozilla developers Christoph Kerschbaumer, Olli Pettay, Sandor Molnar, and Simon Giesecke reported memory safety bugs

present in Firefox 90 and Firefox ESR 78.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29989) - Mozilla developers and community members Kershaw Chang, Philipp, Chris Peterson, and Sebastian Hengst reported memory safety bugs present in Firefox 90. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29990) 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 Mozilla Firefox version 91.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2021-33/

58. Mozilla Firefox Less-than 92.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 92.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-38 advisory. - Firefox for Android allowed navigations through the `intent://` protocol, which could be used to cause crashes and UI spoofs. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29993) - Mixed-content checks were unable to analyze opaque origins which led to some mixed content being loaded. (CVE-2021-38491) - When delegating navigations to the operating system, Firefox would accept the `mk` scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. This bug only affects Firefox for Windows. Other operating systems are unaffected. (CVE-2021-38492) - Mozilla developers Gabriele Svelto and Tyson Smith reported memory safety bugs present in Firefox 91 and Firefox ESR 78.13. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-38493) - Mozilla developers Christian Holler and Lars T Hansen reported memory safety bugs present in Firefox 91. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have

been exploited to run arbitrary code. (CVE-2021-38494) 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 Mozilla Firefox version 92.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2021-38/

59. Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU): The remote host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

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

60. Insecure Windows Service Permissions: At least one improperly configured Windows service may have a privilege escalation vulnerability.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS4 - (10.10.50.24) - Open

LWDC-VEEAM - (10.10.50.102) - Open

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

61. Oracle Java SE 1.7.0_261 / 1.8.0_251 / 1.11.0_7 / 1.14.0_1 Multiple Vulnerabilities (Apr 2020 CPU): The remote host is affected by multiple vulnerabilities

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 261, 8 Update 251, 11 Update 7, or 14 Update 1. It is, therefore, affected by multiple vulnerabilities related to the following components : - Oracle Java SE and Java SE Embedded are prone to a buffer overflow attack, over 'Multiple' protocol. This issue affects the 'JavaFX (libxslt)' component. Successful attacks of this vulnerability allow unauthenticated attacker with network access to takeover of Java SE. (CVE-2019-18197) - Oracle Java SE and Java SE Embedded are prone to partial denial of service (partial DOS) vulnerability. An unauthenticated remote attacker can exploit this over 'Multiple' protocol. This issue affects the 'Scripting' component. (CVE-2020-2754, CVE-2020-2755) - Oracle Java SE and Java SE Embedded are prone to partial denial of service (partial DOS) vulnerability. An unauthenticated remote attacker can exploit this over 'Multiple' protocol. This issue affects the 'Serialization' component. (CVE-2020-2756, CVE-2020-2757) - Oracle Java SE prone to unauthorized read access vulnerability. An unauthenticated remote attacker can exploit this over 'Multiple' protocol can result in unauthorized read access to a subset of Java SE accessible data. This issue affects the 'Advanced Management Console' component. (CVE-2020-2764) - Oracle Java SE and Java SE Embedded are prone to unauthorized write/read access vulnerability. An unauthenticated remote attacker over 'HTTPS' can read, update, insert or delete access to some of Java SE accessible data. This issue affects the 'JSSE' component. (CVE-2020-2767) - Oracle Java SE and Java SE Embedded are prone to partial denial of service

(partial DOS) vulnerability. An unauthenticated remote attacker can exploit this over 'Multiple' protocol. This issue affects the 'Scripting' component. (CVE-2020-2773) It is also affected by other vulnerabilities; please see vendor advisories for more information. 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 Oracle JDK / JRE 14 Update 1 , 11 Update 7, 8 Update 251 , 7 Update 261 or later. If necessary, remove any affected versions.
https://www.oracle.com/a/tech/docs/cpuapr2020cvrf.xml https://www.oracle.com/security-alerts/cpuapr2020.html

62. Oracle Java SE 1.7.0_271 / 1.8.0_261 / 1.11.0_8 / 1.14.0_2 Multiple Vulnerabilities (Jul 2020 CPU): The remote host is affected by multiple vulnerabilities

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 271, 8 Update 261, 11 Update 8, or 14 Update 2. It is, therefore, affected by multiple vulnerabilities related to the following components as referenced in the July 2020 CPU advisory: - Vulnerability in the Java SE product of Oracle Java SE (component: JavaFX). The supported version that is affected is Java SE: 8u251. 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 and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: 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-2020-14664) - Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to

compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: 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-2020-14583) - Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: 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-2020-14593) 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 July 2020 Oracle Critical Patch Update advisory. https://www.oracle.com/a/tech/docs/cpujul2020cvrf.xml https://www.oracle.com/security-alerts/cpujul2020.html

63. Windows Security Feature Bypass in Secure Boot (BootHole): The remote Windows host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

NFINIT-UTIL01 - (10.10.101.101) - Open

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 14, 2023 DBX update referenced in the vendor advisory.

Solution

Refer to the vendor advisory for guidance.
http://www.nessus.org/u?6f75665a http://www.nessus.org/u?840ba26f

64. Oracle Java SE 1.7.0_251 / 1.8.0_241 / 1.11.0_6 / 1.13.0_2 Multiple Vulnerabilities (Jan 2020 CPU): The remote Windows host contains a programming platform that is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 251, 8 Update 241, 11 Update 6, or 13 Update 2. It is, therefore, affected by multiple vulnerabilities: - Oracle Java SE and Java SE Embedded are prone to a severe division by zero, over 'Multiple' protocol. This issue affects the 'SQLite' component.(CVE-2019-16168) - Oracle Java SE and Java SE Embedded are prone to format string vulnerability, leading to a read uninitialized stack data over 'Multiple' protocol. This issue affects the 'libxst' component. (CVE-2019-13117, CVE-2019-13118) - Oracle Java SE and Java SE Embedded are prone to a remote security

vulnerability. An unauthenticated remote attacker can exploit this over 'Kerberos' protocol. This issue affects the 'Security' component. (CVE-2020-2601, CVE-2020-2590) - Oracle Java SE/Java SE Embedded are prone to a remote security vulnerability. An unauthenticated remote attacker can exploit this overmultiple protocols. This issue affects the 'Serialization' component. (CVE-2020-2604, CVE-2020-2583) - Oracle Java SE/Java SE Embedded are prone to a remote security vulnerability. Tn unauthenticated remote attacker can exploit this over multiple protocols. This issue affects the 'Networking' component. (CVE-2020-2593, CVE-2020-2659) - Oracle Java SE are prone to a remote security vulnerability. An unauthenticated remote attacker can exploit this over multiple protocols. This issue affects the 'Libraries' component. (CVE-2020-2654) - Oracle Java SE are prone to a multiple security vulnerability. An unauthenticated remote attacker can exploit this over multiple protocols. This issue affects the 'JavaFX' component. (CVE-2020-2585) - Oracle Java SE are prone to a multiple security vulnerability. An unauthenticate remote attacker can exploit this over 'HTTPS' protocols. This issue affects the 'JSSE' component. (CVE-2020-2655) Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Oracle JDK / JRE 13 Update 2 , 11 Update 6, 8 Update 241 / 7 Update 251 or later. If necessary, remove any affected versions.
http://www.nessus.org/u?d22a1e87

65. Mozilla Firefox Less-than 89.0.1: A web browser installed on the remote Windows host is affected by a vulnerability.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 89.0.1. It is, therefore, affected by a vulnerability as referenced in the mfsa2021-27 advisory. - When drawing text onto a canvas with WebRender disabled, an out of bounds read could occur. This bug only affects Firefox on Windows. Other operating systems are unaffected. (CVE-2021-29968) 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 Mozilla Firefox version 89.0.1 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2021-27/

66. Mozilla Firefox Less-than 91.0.1: A web browser installed on the remote Windows host is affected by a vulnerability.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 91.0.1. It is, therefore, affected by a vulnerability as referenced in the mfsa2021-37 advisory. - Firefox incorrectly accepted a newline in a HTTP/3 header, interpretting it as two separate headers. This allowed for a header splitting attack against servers using HTTP/3. (CVE-2021-29991) 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 Mozilla Firefox version 91.0.1 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2021-37/

67. Security Updates for Microsoft ASP.NET Core (December 2021): The Microsoft ASP.NET Core installations on the remote host are missing a security update.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The Microsoft ASP.NET Core installations on the remote host are missing a security update. It is, therefore, affected by an elevation of privilege vulnerability. An attacker can exploit this to gain elevated privileges. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update ASP.NET Core, remove vulnerable packages and refer to vendor advisory.
https://github.com/dotnet/announcements/issues/206
https://github.com/dotnet/aspnetcore/issues/39028

68. Security Updates for Microsoft .NET Core (October 2022): The Microsoft .NET core installations on the remote host are affected by a privilege escalation vulnerability.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

A privilege escalation vulnerability exists in .NET core 6.0 Less-than 6.0.10 and .NET Core 3.1 Less-than 3.1.30. An authenticated, local attacker can exploit this, via the NuGet client, to cause the user to execute arbitrary code. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update .NET Core Runtime to version 3.1.30 or 6.0.10.
https://support.microsoft.com/help/5019349 https://support.microsoft.com/help/5019351
https://dotnet.microsoft.com/download/dotnet/3.1 https://dotnet.microsoft.com/download/dotnet/6.0
http://www.nessus.org/u?1a5250e3 http://www.nessus.org/u?0eafd070
https://github.com/dotnet/core/issues/7864

69. Adobe Reader Less-than 20.005.30467 / 23.001.20143 Multiple Vulnerabilities (APSB23-24): The version of Adobe Reader installed on the remote Windows host is

affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

CIT-PWS - (10.10.50.20) - Open

Description

The version of Adobe Reader installed on the remote Windows host is a version prior to 20.005.30467 or 23.001.20143. It is, therefore, affected by multiple vulnerabilities. - Out-of-bounds Write (CWE-787) potentially leading to Arbitrary code execution (CVE-2023-26395) - Violation of Secure Design Principles (CWE-657) potentially leading to Privilege escalation (CVE-2023-26396) - Out-of-bounds Read (CWE-125) potentially leading to Memory leak (CVE-2023-26397) - Improper Input Validation (CWE-20) potentially leading to Arbitrary code execution (CVE-2023-26405, CVE-2023-26407) - Improper Access Control (CWE-284) potentially leading to Security feature bypass (CVE-2023-26406, CVE-2023-26408) - Use After Free (CWE-416) potentially leading to Arbitrary code execution (CVE-2023-26417, CVE-2023-26418, CVE-2023-26419, CVE-2023-26420, CVE-2023-26422, CVE-2023-26423, CVE-2023-26424) - Integer Underflow (Wrap or Wraparound) (CWE-191) potentially leading to Arbitrary code execution (CVE-2023-26421) - Out-of-bounds Read (CWE-125) potentially leading to Arbitrary code execution (CVE-2023-26425) 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 20.005.30467 / 23.001.20143 or later.
https://helpx.adobe.com/security/products/acrobat/apsb23-24.html

70. Oracle Java SE Multiple Vulnerabilities (April 2023 CPU): The remote host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

CITS7 - (10.10.50.27) - Open

LWDC-VEEAM - (10.10.50.102) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is affected by multiple vulnerabilities as referenced in the April 2023 CPU advisory: - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2023-21930) - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2023-21939) - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2023-21954) 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 April 2023 Oracle Critical Patch Update advisory.
https://www.oracle.com/docs/tech/security-alerts/cpuapr2023cvrf.xml
https://www.oracle.com/security-alerts/cpuapr2023.html#AppendixJAVA

71. Adobe Reader Less-than 20.005.30407 / 22.003.20258 Multiple Vulnerabilities (APSB22-46): The version of Adobe Reader installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-PWS - (10.10.50.20) - Open

Description

The version of Adobe Reader installed on the remote Windows host is a version prior to 20.005.30407 or 22.003.20258. It is, therefore, affected by multiple vulnerabilities. - Adobe Acrobat Reader versions 22.002.20212 (and earlier) and 20.005.30381 (and earlier) are affected by a Stack-based Buffer Overflow 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-2022-38450, CVE-2022-42339) - Adobe Acrobat Reader versions 22.002.20212 (and earlier) and 20.005.30381 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. (CVE-2022-35691) - Adobe Acrobat Reader versions 22.002.20212 (and earlier) and 20.005.30381 (and earlier) are affected by a Use After Free 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-2022-38437) - Adobe Acrobat Reader versions 22.002.20212 (and earlier) and 20.005.30381 (and earlier) are affected by an out-of-bounds read 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-2022-38449, CVE-2022-42342) 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 20.005.30407 / 22.003.20258 or later.
https://helpx.adobe.com/security/products/acrobat/apsb22-46.html

72. Adobe Reader Less-than 20.005.30436 / 22.003.20310 Multiple Vulnerabilities (APSB23-01): The version of Adobe Reader installed on the remote Windows host is

affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-PWS - (10.10.50.20) - Open

Description

The version of Adobe Reader installed on the remote Windows host is a version prior to 20.005.30436 or 22.003.20310. It is, therefore, affected by multiple vulnerabilities. - Adobe Acrobat Reader versions 22.002.20212 (and earlier) and 20.005.30381 (and earlier) are affected by a Use After Free 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-2022-38437) - Integer Overflow or Wraparound (CWE-190) potentially leading to Arbitrary code execution (CVE-2023-21579) - Out-of-bounds Read (CWE-125) potentially leading to Memory Leak (CVE-2023-21581, CVE-2023-21585) - NULL Pointer Dereference (CWE-476) potentially leading to Application denial-of-service (CVE-2023-21586) - Stack-based Buffer Overflow (CWE-121) potentially leading to Arbitrary code execution (CVE-2023-21604, CVE-2023-21610) - Heap-based Buffer Overflow (CWE-122) potentially leading to Arbitrary code execution (CVE-2023-21605) - Out-of-bounds Write (CWE-787) potentially leading to Arbitrary code execution (CVE-2023-21606, CVE-2023-21609) - Improper Input Validation (CWE-20) potentially leading to Arbitrary code execution (CVE-2023-21607) - Use After Free (CWE-416) potentially leading to Arbitrary code execution (CVE-2023-21608) - Violation of Secure Design Principles (CWE-657) potentially leading to Privilege escalation (CVE-2023-21611, CVE-2023-21612) - Out-of-bounds Read (CWE-125) potentially leading to Memory leak (CVE-2023-21613, CVE-2023-21614) 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 20.005.30436 / 22.003.20310 or later.
https://helpx.adobe.com/security/products/acrobat/apsb23-01.html

73. Microsoft Windows Unquoted Service Path Enumeration: The remote Windows host has at least one service installed that uses an unquoted service path.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

CITS4 - (10.10.50.24) - Open

CITS7 - (10.10.50.27) - Open

CIT-TECH - (10.40.50.97) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The remote Windows host has at least one service installed that uses an unquoted service path, which contains at least one whitespace. A local attacker can gain elevated privileges by inserting an executable file in the path of the affected service. Note that this is a generic test that will flag any application affected by the described vulnerability.

Solution

Ensure that any services that contain a space in the path enclose the path in quotes.
http://www.nessus.org/u?84a4cc1c http://cwe.mitre.org/data/definitions/428.html https://www.commonexploits.com/unquoted-service-paths/ http://www.nessus.org/u?4aa6acbc

74. Security Updates for Microsoft .NET Framework (February 2023): The Microsoft .NET Framework installation on the remote host is missing a security update.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS8 - (10.10.50.28) - Open

Description

The Microsoft .NET Framework installation on the remote host is missing a security update. It is, therefore, affected by multiple vulnerabilities, as follows: - A denial of service (DoS) vulnerability. (CVE-2023-21722) - A remote code execution vulnerability. (CVE-2023-21808)

Solution

Microsoft has released security updates for Microsoft .NET Framework.
http://www.nessus.org/u?5bd7d30c http://www.nessus.org/u?42dae88f
http://www.nessus.org/u?db0b1765 https://support.microsoft.com/en-us/help/5022497
https://support.microsoft.com/en-us/help/5022498 https://support.microsoft.com/en-us/help/5022499
https://support.microsoft.com/en-us/help/5022501 https://support.microsoft.com/en-us/help/5022502
https://support.microsoft.com/en-us/help/5022503 https://support.microsoft.com/en-us/help/5022504
https://support.microsoft.com/en-us/help/5022505 https://support.microsoft.com/en-us/help/5022506
https://support.microsoft.com/en-us/help/5022507 https://support.microsoft.com/en-us/help/5022508
https://support.microsoft.com/en-us/help/5022509 https://support.microsoft.com/en-us/help/5022511
https://support.microsoft.com/en-us/help/5022512 https://support.microsoft.com/en-us/help/5022513
https://support.microsoft.com/en-us/help/5022514 https://support.microsoft.com/en-us/help/5022515
https://support.microsoft.com/en-us/help/5022516 https://support.microsoft.com/en-us/help/5022520
https://support.microsoft.com/en-us/help/5022521 https://support.microsoft.com/en-us/help/5022522
https://support.microsoft.com/en-us/help/5022523 https://support.microsoft.com/en-us/help/5022524
https://support.microsoft.com/en-us/help/5022525 https://support.microsoft.com/en-us/help/5022526
https://support.microsoft.com/en-us/help/5022529 https://support.microsoft.com/en-us/help/5022530
https://support.microsoft.com/en-us/help/5022531 https://support.microsoft.com/en-us/help/5022574
https://support.microsoft.com/en-us/help/5022575

75. Microsoft Teams Less-than 1.3.0.13000 Remote Code Execution: The version of Microsoft Teams installed on the remote Windows host is affected by a remote code execution vulnerability.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of Microsoft Teams installed on the remote Windows host is a version prior to 1.3.0.13000. It is, therefore, affected by remote code execution vulnerability. 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 Microsoft Teams 1.3.0.13000 or later.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17091

76. Security Updates for Microsoft .NET core (May 2022): The Microsoft .NET core installations on the remote host are affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The Microsoft .NET core installations on the remote host are missing security updates. It is, therefore, affected by multiple denial of service vulnerabilities: - A vulnerability where a malicious client can cause a denial of service via excess memory allocations through HttpClient. (CVE-2022-23267) - A vulnerability where a malicious client can manipulate cookies and cause a denial of service. (CVE-2022-29117) - A vulnerability where a malicious client can cause a denial of service when HTML forms are parsed. (CVE-2022-29145) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update .NET Core Runtime to version 3.1.25, 5.0.17 or 6.0.5.
https://dotnet.microsoft.com/download/dotnet/3.1 https://dotnet.microsoft.com/download/dotnet/5.0 https://dotnet.microsoft.com/download/dotnet/6.0
https://github.com/dotnet/announcements/issues/219 http://www.nessus.org/u?3b99f604 http://www.nessus.org/u?b1b0aff4 http://www.nessus.org/u?39d07c32

77. Security Updates for Microsoft ASP.NET Core (September 2022): The Microsoft

ASP.NET Core installations on the remote host are missing a security update.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

A denial of service vulnerability exists in ASP.NET core 6.0 Less-than 6.0.9 and ASP.NET Core 3.1 Less-than 3.1.29. An unauthenticated, remote attacker can exploit this, by sending a customized payload that is parsed during model binding, to cause a stack overflow, which may cause the application to stop responding. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update ASP.NET Core Runtime to version 3.1.29 or 6.0.9.
https://github.com/dotnet/announcements/issues/234 http://www.nessus.org/u?c76821a3

78. Security Updates for Microsoft .NET Core (September 2022): The Microsoft .NET core installations on the remote host are affected by a denial of service vulnerability.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

A denial of service vulnerability exists in .NET core 6.0 Less-than 6.0.9 and .NET Core 3.1 Less-than 3.1.29. An unauthenticated, remote attacker can exploit this, by sending a customized payload that is

parsed during model binding, to cause a stack overflow, which may cause the application to stop responding. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update .NET Core Runtime to version 3.1.29 or 6.0.9.
https://support.microsoft.com/help/5017903 https://support.microsoft.com/help/5017915
https://dotnet.microsoft.com/download/dotnet/3.1 https://dotnet.microsoft.com/download/dotnet/6.0
http://www.nessus.org/u?cf2fdae6 http://www.nessus.org/u?775af4a9
https://github.com/dotnet/core/issues/7791

79. DNS Server Spoofed Request Amplification DDoS: The remote DNS server could be used in a distributed denial of service attack.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

- (70.167.3.1) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

Description

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

Solution

Restrict access to your DNS server from public network or reconfigure it to reject such queries.
https://isc.sans.edu/diary/DNS+queries+for+/5713

80. Mozilla Firefox Less-than 112.0: A web browser installed on the remote Windows host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

CIT-TECH - (10.40.50.97) - Open

Description

The version of Firefox installed on the remote Windows host is prior to 112.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2023-13 advisory. - An attacker could have caused an out of bounds memory access using WebGL APIs, leading to memory corruption and a potentially exploitable crash. This bug only affects Firefox for macOS. Other operating systems are unaffected. (CVE-2023-29531) - A local attacker can trick the Mozilla Maintenance Service into applying an unsigned update file by pointing the service at an update file on a malicious SMB server. The update file can be replaced after the signature check, before the use, because the write-lock requested by the service does not work on a SMB server. Note: This attack requires local system access and only affects Windows. Other operating systems are not affected. (CVE-2023-29532) - A website could have obscured the fullscreen notification by using a combination of Less-thancodeGreater-thanwindow.openLess-than/codeGreater-than, fullscreen requests, Less-thancodeGreater-thanwindow.nameLess-than/codeGreater-than assignments, and Less-thancodeGreater-thansetIntervalLess-than/codeGreater-than calls. This could have led to user confusion and possible spoofing attacks. (CVE-2023-29533) - Different techniques existed to obscure the fullscreen notification in Firefox and Focus for Android. These could have led to potential user confusion and spoofing attacks. This bug only affects Firefox and Focus for Android. Other versions of Firefox are unaffected. (CVE-2023-29534) - Following a Garbage Collector compaction, weak maps may have been accessed before they were correctly traced. This resulted in memory corruption and a potentially exploitable crash. (CVE-2023-29535) - An attacker could cause the memory manager to incorrectly free a pointer that addresses attacker- controlled memory, resulting in an assertion, memory corruption, or a potentially exploitable crash. (CVE-2023-29536) - Multiple race conditions in the font initialization could have led to memory corruption and execution of attacker-controlled code. (CVE-2023-29537) - Under specific circumstances a WebExtension may have received a Less-thancodeGreater-thanjar:file:///Less-than/codeGreater-than URI instead of a Less-thancodeGreater-thanmoz-extension:///Less-than/codeGreater-than URI during a load request. This leaked directory paths on the user's machine. (CVE-2023-29538) - When handling the filename

directive in the Content-Disposition header, the filename would be truncated if the filename contained a NULL character. This could have led to reflected file download attacks potentially tricking users to install malware. (CVE-2023-29539) - Using a redirect embedded into Less-thancodeGreater-thansourceMappingUrlsLess-than/codeGreater-than could allow for navigation to external protocol links in sandboxed iframes without Less-thancodeGreater-thanallow-top-navigation-to-custom-protocolsLess-than/codeGreater-than. (CVE-2023-29540) - Firefox did not properly handle downloads of files ending in Less-thancodeGreater-than.desktopLess-than/codeGreater-than, which can be interpreted to run attacker-controlled commands. This bug only affects Firefox for Linux on certain Distributions. Other operating systems are unaffected, and Mozilla is unable to enumerate all affected Linux Distributions. (CVE-2023-29541) - A newline in a filename could have been used to bypass the file extension security mechanisms that replace malicious file extensions such as .lnk with .download. This could have led to accidental execution of malicious code. This bug only affects Firefox on Windows. Other versions of Firefox are unaffected. (CVE-2023-29542) - An attacker could have caused memory corruption and a potentially exploitable use-after-free of a pointer in a global object's debugger vector. (CVE-2023-29543) - If multiple instances of resource exhaustion occurred at the incorrect time, the garbage collector could have caused memory corruption and a potentially exploitable crash. (CVE-2023-29544) - Similar to CVE-2023-28163, this time when choosing 'Save Link As', suggested filenames containing environment variable names would have resolved those in the context of the current user. This bug only affects Firefox on Windows. Other versions of Firefox are unaffected. (CVE-2023-29545) - When recording the screen while in Private Browsing on Firefox for Android the address bar and keyboard were not hidden, potentially leaking sensitive information. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2023-29546) - When a secure cookie existed in the Firefox cookie jar an insecure cookie for the same domain could have been created, when it should have silently failed. This could have led to a desynchronization in expected results when reading from the secure cookie. (CVE-2023-29547) - A wrong lowering instruction in the ARM64 Ion compiler resulted in a wrong optimization result. (CVE-2023-29548) - Under certain circumstances, a call to the Less-thancodeGreater-thanbindLess-than/codeGreater-than function may have resulted in the incorrect realm. This may have created a vulnerability relating to JavaScript-implemented sandboxes such as SES. (CVE-2023-29549) - Mozilla developers Randell Jesup, Andrew Osmond, Sebastian Hengst, Andrew McCreight, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 111 and Firefox ESR 102.9. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2023-29550) - Mozilla developers Randell Jesup, Andrew McCreight, Gabriele Svelto, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 111. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2023-29551) 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 Mozilla Firefox version 112.0 or later.
https://www.mozilla.org/en-US/security/advisories/mfsa2023-13/

81. SSL Certificate Signed Using Weak Hashing Algorithm: An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-Azure-VBO - (10.1.1.4) - Open

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CIT-FLEX-HPE - (10.10.50.65) - Open

cit-android - (10.10.50.115) - Open

CLOUDS1 - (10.20.66.10) - Open

CIT-TECH - (10.40.50.97) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

https://tools.ietf.org/html/rfc3279 http://www.nessus.org/u?9bb87bf2 http://www.nessus.org/u?e120eea1 http://www.nessus.org/u?5d894816 http://www.nessus.org/u?51db68aa http://www.nessus.org/u?9dc7bfba

82. SSL Medium Strength Cipher Suites Supported (SWEET32): The remote service supports the use of medium strength SSL ciphers.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-Azure-VBO - (10.1.1.4) - Open

CIT-SQL - (10.10.50.13) - Open

CIT-ARCH - (10.10.50.14) - Open

CIT-SC - (10.10.50.15) - Open

CIT-PWS - (10.10.50.20) - Open

CITS1 - (10.10.50.21) - Open

cIT-RDS - (10.10.50.22) - Open

CITS4 - (10.10.50.24) - Open

CIT-MGMT - (10.10.50.25) - Open

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CIT-FS - (10.10.50.30) - Open

CIT-APOLLO - (10.10.50.31) - Open

CIT-ROOT-CA - (10.10.50.32) - Open

CIT-FLEX-HPE - (10.10.50.65) - Open

ReportManager - (10.10.50.71) - Open

LWDC-VEEAM - (10.10.50.102) - Open

cit-android - (10.10.50.115) - Open

NFINIT-VBR - (10.10.102.100) - Open

CLOUDS1 - (10.20.66.10) - Open

CIT-TECH - (10.40.50.97) - Open

CIT-PROVISIONING - (10.40.51.12) - Open

- (70.167.3.15) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

- (70.167.3.71) - Open

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.
https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info

83. Oracle Java SE 1.7.0_311 / 1.8.0_301 / 1.11.0_12 / 1.16.0_2 Multiple Vulnerabilities (July 2021 CPU): The remote host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 301, 8 Update 291, 11 Update 11, or 16 Update 1. It is, therefore, affected by multiple vulnerabilities as referenced in the July 2021 CPU advisory: - Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition 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-2021-2341) - Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Library). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition 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-2021-2369) - Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle

GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE, Oracle GraalVM Enterprise Edition. 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-2021-2388) - Vulnerability in the Java SE product of Oracle Java SE (component: JNDI). The supported version that is affected is Java SE: 7u301. Difficult to exploit 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 partial denial of service (partial DOS) 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2021-2432) 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 July 2021 Oracle Critical Patch Update advisory. https://www.oracle.com/a/tech/docs/cpujul2021cvrf.xml https://www.oracle.com/security-alerts/cpujul2021.html#AppendixJAVA

84. Oracle Java SE Multiple Vulnerabilities (April 2022 CPU): The remote host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is affected by multiple vulnerabilities as referenced in the April 2022 CPU advisory: - Vulnerability in the

Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 17.0.2 and 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21449) - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21476) - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21426) 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 April 2022 Oracle Critical Patch Update advisory. https://www.oracle.com/a/tech/docs/cpuapr2022cvrf.xml https://www.oracle.com/security-alerts/cpuapr2022.html#AppendixJAVA

85. Oracle Java SE Multiple Vulnerabilities (July 2022 CPU): The remote host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is affected by multiple vulnerabilities as referenced in the July 2022 CPU advisory: - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-21540) - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-21541) - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 17.0.3.1; Oracle GraalVM Enterprise Edition: 21.3.2 and 22.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-21549) - Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Native Image (Gson)). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle GraalVM Enterprise Edition executes to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GraalVM Enterprise Edition. (CVE-2022-25647) - Vulnerability in the Oracle Java SE, Oracle

GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP (Xalan-J)). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-34169) 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 July 2022 Oracle Critical Patch Update advisory. https://www.oracle.com/docs/tech/security-alerts/cpujul2022cvrf.xml https://www.oracle.com/security-alerts/cpujul2022.html#AppendixJAVA

86. Security Updates for Internet Explorer (September 2017): The Internet Explorer installation on the remote host is affected by multiple vulnerabilities.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The Internet Explorer installation on the remote host is missing security updates. It is, therefore, affected by multiple vulnerabilities : - An information disclosure vulnerability exists when affected Microsoft scripting engines do not properly handle objects in memory. The vulnerability could allow an attacker to detect specific files on the user's computer. (CVE-2017-8529) - A remote code execution vulnerability exists when Microsoft browsers improperly access objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8750) - A spoofing vulnerability exists when Internet Explorer improperly handles specific HTML content. An attacker who successfully exploited this vulnerability could trick a user into believing that the user was visiting a legitimate website. The specially crafted website could

either spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services. (CVE-2017-8733) - A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. (CVE-2017-8747, CVE-2017-8749) - A remote code execution vulnerability exists in the way that Microsoft browser JavaScript engines render content when handling objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the related rendering engine. The attacker could also take advantage of compromised websites, and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. (CVE-2017-8741, CVE-2017-8748) - An information disclosure vulnerability exists in Microsoft browsers due to improper parent domain verification in certain functionality. An attacker who successfully exploited the vulnerability could obtain specific information that is used in the parent domain. (CVE-2017-8736)

Solution

Microsoft has released security updates for the affected versions of Internet Explorer.
http://www.nessus.org/u?26b484bb http://www.nessus.org/u?085e4d22 http://www.nessus.org/u?35364720 http://www.nessus.org/u?1dbb18cc

87. Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104): A package installed on the remote host is affected by a remote code execution vulnerability.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-FS - (10.10.50.30) - Open

CIT-TECH - (10.40.50.97) - Open

Description

The version of Apache Log4j on the remote host is 1.2. It is, therefore, affected by a remote code execution vulnerability when specifically configured to use JMSAppender. 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 Apache Log4j version 2.16.0 or later since 1.x is end of life. 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.
http://www.nessus.org/u?33485eac https://access.redhat.com/security/cve/CVE-2021-4104

88. Security Update for .NET Core (August 2021): The remote Windows host is affected by a .NET Core denial of service (DoS) vulnerability.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The Microsoft .NET Core installation on the remote host is version 2.1.x prior to 2.1.29, 3.1.x prior to 3.1.18, or 5.x prior to 5.0.9. It is, therefore affected by a denial of service (DoS) vulnerability, as server applications providing WebSocket endpoints can be tricked into endlessly looping while trying to read a single WebSocket frame. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update .NET Core, remove vulnerable packages and refer to vendor advisory.
https://dotnet.microsoft.com/download/dotnet/2.1 https://dotnet.microsoft.com/download/dotnet-core/3.1 https://dotnet.microsoft.com/download/dotnet/5.0 http://www.nessus.org/u?8ff12246 http://www.nessus.org/u?0933ffe1 http://www.nessus.org/u?6242d65f https://devblogs.microsoft.com/dotnet/net-august-2021/

89. WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck): The remote Windows host is potentially missing a mitigation for a remote code execution vulnerability.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-SQL - (10.10.50.13) - Open

CIT-ARCH - (10.10.50.14) - Open

CIT-SC - (10.10.50.15) - Open

CIT-PWS - (10.10.50.20) - Open

CITS1 - (10.10.50.21) - Open

cIT-RDS - (10.10.50.22) - Open

cit-mrtg - (10.10.50.23) - Open

CITS4 - (10.10.50.24) - Open

CIT-MGMT - (10.10.50.25) - Open

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CIT-FS - (10.10.50.30) - Open

CIT-APOLLO - (10.10.50.31) - Open

CIT-ROOT-CA - (10.10.50.32) - Open

ReportManager - (10.10.50.71) - Open

LWDC-VEEAM - (10.10.50.102) - Open

NFINIT-UTIL01 - (10.10.101.101) - Open

CIT-TECH - (10.40.50.97) - Open

- (70.167.3.15) - Open

CITS7 - WAN - (70.167.3.27) - Open

- (70.167.3.71) - Open

Description

The remote system may be in a vulnerable state to CVE-2013-3900 due to a missing or misconfigured registry keys: - HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck An unauthenticated, remote attacker could exploit this, by sending specially crafted requests, to execute arbitrary code on an affected host.

Solution

Add and enable registry value EnableCertPaddingCheck: - HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck Additionally, on 64 Bit OS systems, Add and enable registry value EnableCertPaddingCheck: - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900
http://www.nessus.org/u?9780b9d2

90. Untrusted Microsoft Office Macro Execution Enabled: A Microsoft Office application installed on the remote host has untrusted macro execution settings enabled.

Severity	High	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

Description

A Microsoft Office application installed on the remote host has untrusted macro execution settings enabled. Note: This plugin first checks to verify that there are any Microsoft Office products actually installed. If there are, it will enumerate the registry keys that are set when an Office application allows the execution of untrusted macros. In some in edge cases, the registry settings that allow the execution of untrusted macros may still be present and set, even if there are no installed Microsoft Office products. In this scenario, this plugin will require paranoid mode to check these registry keys.

Solution

Disable the macro execution trust settings.

91. SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE): It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-SQL - (10.10.50.13) - Open

CITS8 - (10.10.50.28) - Open

CIT-TECH - (10.40.50.97) - Open

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service. The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism. This is a vulnerability in the SSLv3 specification, not in any particular SSL

implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Solution

Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.
https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

92. SSL Certificate Cannot Be Trusted: The SSL certificate for this service cannot be trusted.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-Azure-VBO - (10.1.1.4) - Open

CIT-SQL - (10.10.50.13) - Open

CIT-ARCH - (10.10.50.14) - Open

CIT-SC - (10.10.50.15) - Open

CITS1 - (10.10.50.21) - Open

cIT-RDS - (10.10.50.22) - Open

CITS4 - (10.10.50.24) - Open

CIT-MGMT - (10.10.50.25) - Open

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CIT-FS - (10.10.50.30) - Open

CIT-APOLLO - (10.10.50.31) - Open

CIT-ROOT-CA - (10.10.50.32) - Open

CIT-FLEX-HPE - (10.10.50.65) - Open

ReportManager - (10.10.50.71) - Open

LWDC-VEEAM - (10.10.50.102) - Open

cit-android - (10.10.50.115) - Open

NFINIT-VBR - (10.10.102.100) - Open

CLOUDS1 - (10.20.66.10) - Open

CIT-TECH - (10.40.50.97) - Open

CIT-PROVISIONING - (10.40.51.12) - Open

- (70.167.3.15) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

- (70.167.3.71) - Open

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support

or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.
https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509

93. SSL Self-Signed Certificate: The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-Azure-VBO - (10.1.1.4) - Open

CIT-SQL - (10.10.50.13) - Open

CIT-ARCH - (10.10.50.14) - Open

CIT-SC - (10.10.50.15) - Open

CITS1 - (10.10.50.21) - Open

cIT-RDS - (10.10.50.22) - Open

CITS4 - (10.10.50.24) - Open

CIT-MGMT - (10.10.50.25) - Open

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CIT-FS - (10.10.50.30) - Open

CIT-ROOT-CA - (10.10.50.32) - Open

CIT-FLEX-HPE - (10.10.50.65) - Open

LWDC-VEEAM - (10.10.50.102) - Open

cit-android - (10.10.50.115) - Open

NFINIT-VBR - (10.10.102.100) - Open

CLOUDS1 - (10.20.66.10) - Open

CIT-TECH - (10.40.50.97) - Open

CIT-PROVISIONING - (10.40.51.12) - Open

- (70.167.3.15) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

94. TLS Version 1.0 Protocol Detection: The remote service encrypts traffic using an older version of TLS.

Severity	Medium	Status	Open

First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-Azure-VBO - (10.1.1.4) - Open

CIT-SQL - (10.10.50.13) - Open

CIT-ARCH - (10.10.50.14) - Open

CIT-SC - (10.10.50.15) - Open

CIT-PWS - (10.10.50.20) - Open

CITS1 - (10.10.50.21) - Open

CITS4 - (10.10.50.24) - Open

CIT-MGMT - (10.10.50.25) - Open

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CIT-FS - (10.10.50.30) - Open

CIT-APOLLO - (10.10.50.31) - Open

CIT-ROOT-CA - (10.10.50.32) - Open

CIT-FLEX-HPE - (10.10.50.65) - Open

ReportManager - (10.10.50.71) - Open

LWDC-VEEAM - (10.10.50.102) - Open

cit-android - (10.10.50.115) - Open

CIT-SFTP - (10.10.101.32) - Open

NFINIT-VBR - (10.10.102.100) - Open

CLOUDS1 - (10.20.66.10) - Open

CIT-TECH - (10.40.50.97) - Open

CIT-PROVISIONING - (10.40.51.12) - Open

- (70.167.3.15) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

- (70.167.3.71) - Open

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren?t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

95. TLS Version 1.1 Protocol Deprecated: The remote service encrypts traffic using an older version of TLS.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-Azure-VBO - (10.1.1.4) - Open

CIT-SQL - (10.10.50.13) - Open

CIT-ARCH - (10.10.50.14) - Open

CIT-SC - (10.10.50.15) - Open

CIT-PWS - (10.10.50.20) - Open

CITS1 - (10.10.50.21) - Open

cIT-RDS - (10.10.50.22) - Open

CITS4 - (10.10.50.24) - Open

CIT-MGMT - (10.10.50.25) - Open

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CIT-FS - (10.10.50.30) - Open

CIT-APOLLO - (10.10.50.31) - Open

CIT-ROOT-CA - (10.10.50.32) - Open

CIT-FLEX-HPE - (10.10.50.65) - Open

ReportManager - (10.10.50.71) - Open

LWDC-VEEAM - (10.10.50.102) - Open

cit-android - (10.10.50.115) - Open

CIT-SFTP - (10.10.101.32) - Open

NFINIT-VBR - (10.10.102.100) - Open

CLOUDS1 - (10.20.66.10) - Open

CIT-TECH - (10.40.50.97) - Open

CIT-PROVISIONING - (10.40.51.12) - Open

- (70.167.3.15) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

- (70.167.3.71) - Open

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1 As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.
https://datatracker.ietf.org/doc/html/rfc8996 http://www.nessus.org/u?c8ae820d

96. Windows Speculative Execution Configuration Check: The remote host has not properly mitigated a series of speculative execution vulnerabilities.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-SQL - (10.10.50.13) - Open

CIT-PWS - (10.10.50.20) - Open

CITS1 - (10.10.50.21) - Open

cIT-RDS - (10.10.50.22) - Open

cit-mrtg - (10.10.50.23) - Open

CITS4 - (10.10.50.24) - Open

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CIT-FS - (10.10.50.30) - Open

CIT-APOLLO - (10.10.50.31) - Open

ReportManager - (10.10.50.71) - Open

LWDC-VEEAM - (10.10.50.102) - Open

NFINIT-UTIL01 - (10.10.101.101) - Open

CIT-TECH - (10.40.50.97) - Open

CITS7 - WAN - (70.167.3.27) - Open

- (70.167.3.71) - Open

Description

The remote host has not properly mitigated a series of known speculative execution vulnerabilities. It, therefore, may be affected by : - Branch Target Injection (BTI) (CVE-2017-5715) - Bounds Check Bypass (BCB) (CVE-2017-5753) - Rogue Data Cache Load (RDCL) (CVE-2017-5754) - Rogue System Register Read (RSRE) (CVE-2018-3640) - Speculative Store Bypass (SSB) (CVE-2018-3639) - L1 Terminal Fault (L1TF) (CVE-2018-3615, CVE-2018-3620, CVE-2018-3646) - Microarchitectural Data Sampling Uncacheable Memory (MDSUM) (CVE-2019-11091) - Microarchitectural Store Buffer Data Sampling (MSBDS) (CVE-2018-12126) - Microarchitectural Load Port Data Sampling (MLPDS) (CVE-2018-12127) - Microarchitectural Fill Buffer Data Sampling (MFBDS) (CVE-2018-12130) - TSX Asynchronous Abort (TAA) (CVE-2019-11135)

Solution

Apply vendor recommended settings.
http://www.nessus.org/u?8902cebb http://www.nessus.org/u?6a005ed4

97. Windows 10 / Windows Server 2016 September 2017 Information Disclosure Vulnerability (CVE-2017-8529): The remote Windows host is affected by an information disclosure vulnerability.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-SQL - (10.10.50.13) - Open

CIT-PWS - (10.10.50.20) - Open

CITS1 - (10.10.50.21) - Open

cIT-RDS - (10.10.50.22) - Open

cit-mrtg - (10.10.50.23) - Open

CITS4 - (10.10.50.24) - Open

CIT-FS - (10.10.50.30) - Open

CIT-APOLLO - (10.10.50.31) - Open

ReportManager - (10.10.50.71) - Open

LWDC-VEEAM - (10.10.50.102) - Open

CIT-TECH - (10.40.50.97) - Open

- (70.167.3.71) - Open

Description

The remote Windows host is missing a security update or a registry setting required to enable protections for CVE-2017-8529. It is, therefore, affected by an information disclosure vulnerability: - An information disclosure vulnerability exists when affected Microsoft scripting engines do not properly handle objects in memory. The vulnerability could allow an attacker to detect specific files on the user's computer. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability.

Solution

Refer to the Microsoft CVE article for additional information.

http://www.nessus.org/u?1f6a3c24

98. HSTS Missing From HTTPS Server (RFC 6797): The remote web server is not enforcing HSTS, as defined by RFC 6797.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-SQL - (10.10.50.13) - Open

cIT-RDS - (10.10.50.22) - Open

CIT-APOLLO - (10.10.50.31) - Open

CITS7 - (10.10.50.27) - Open

CIT-ROOT-CA - (10.10.50.32) - Open

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Solution

Configure the remote web server to use HSTS.
https://tools.ietf.org/html/rfc6797

99. Remote Desktop Protocol Server Man-in-the-Middle Weakness: It may be possible to get access to the remote host.

Severity	Medium	Status	Open

First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CLOUDS1 - (10.20.66.10) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials. This flaw exists because the RDP server stores a publicly known hard-coded RSA private key. Any attacker in a privileged network location can use the key for this attack.

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and - On Microsoft Windows operating systems, select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.
http://www.nessus.org/u?8033da0d

100. Security Updates for Microsoft SQL Server Reporting Services (September 2020): The Microsoft SQL Server Reporting Services installation on the remote host is missing a security update.

Severity	Medium	Status	Open

First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

ReportManager - (10.10.50.71) - Open

- (70.167.3.71) - Open

Description

The Microsoft SQL Server Reporting Services installation on the remote host is missing a security update. It is, therefore, affected by a security feature bypass vulnerability in SQL Server Reporting Services (SSRS) due to improper validation of uploaded attachments to reports. An authenticated, remote attacker could exploit this issue to upload file types that were disallowed by an administrator. (CVE-2020-1044)

Solution

Refer to Microsoft documentation and upgrade to relevant fixed version.
http://www.nessus.org/u?5708b76b

101. Microsoft Edge (Chromium) Less-than 112.0.1722.34 Multiple Vulnerabilities: The remote host has an web browser installed that is affected by multiple vulnerabilities.

Severity	**Medium**	Status	**Open**
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

CIT-ARCH - (10.10.50.14) - Open

CIT-MGMT - (10.10.50.25) - Open

CITS7 - (10.10.50.27) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 112.0.1722.34. It is, therefore, affected by multiple vulnerabilities as referenced in the April 6, 2023 advisory. - Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability (CVE-2023-28284) - Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2023-24935) - Microsoft Edge (Chromium-based) Tampering Vulnerability (CVE-2023-28301) 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 Microsoft Edge version 112.0.1722.34 or later.
http://www.nessus.org/u?245dfb65 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24935 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28284 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28301

102. JQuery 1.2 Less-than 3.5.0 Multiple XSS: The remote web server is affected by multiple cross site scripting vulnerability.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS7 - (10.10.50.27) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities. Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

Solution

Upgrade to JQuery version 3.5.0 or later.
https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://security.paloaltonetworks.com/PAN-

SA-2020-0007

103. Security Updates for Microsoft .NET Core (August 2022): The Microsoft .NET core installations on the remote host are affected by a spoofing vulnerability.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

A spoofing vulnerability exists in .NET core 6.0 Less-than 6.0.8 and .NET Core 3.1 Less-than 3.1.28. An unauthenticated, remote attacker can exploit this, to perform actions with the privileges of another user. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update .NET Core Runtime to version 3.1.28 or 6.0.8.
https://support.microsoft.com/help/5016987 https://support.microsoft.com/help/5016990 https://dotnet.microsoft.com/download/dotnet/3.1 https://dotnet.microsoft.com/download/dotnet/6.0 http://www.nessus.org/u?327bb1fb http://www.nessus.org/u?7ce182ee https://github.com/dotnet/core/issues/7682

104. SSL RC4 Cipher Suites Supported (Bar Mitzvah): The remote service supports the use of the RC4 cipher.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-SQL - (10.10.50.13) - Open

CIT-PWS - (10.10.50.20) - Open

CITS1 - (10.10.50.21) - Open

cIT-RDS - (10.10.50.22) - Open

CITS4 - (10.10.50.24) - Open

CITS8 - (10.10.50.28) - Open

CIT-FS - (10.10.50.30) - Open

CIT-APOLLO - (10.10.50.31) - Open

ReportManager - (10.10.50.71) - Open

LWDC-VEEAM - (10.10.50.102) - Open

CLOUDS1 - (10.20.66.10) - Open

CIT-TECH - (10.40.50.97) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

- (70.167.3.71) - Open

Description

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
https://www.rc4nomore.com/ http://www.nessus.org/u?ac7327a0 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

105. Curl Use-After-Free Less-than 7.87 (CVE-2022-43552): The remote Windows host has a program that is affected by a use-after-free vulnerability.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-ARCH - (10.10.50.14) - Open

CIT-MGMT - (10.10.50.25) - Open

CIT-ROOT-CA - (10.10.50.32) - Open

CIT-SC - (10.10.50.15) - Closed

NFINIT-UTIL01 - (10.10.101.101) - Closed

- (70.167.3.15) - Closed

Description

The version of Curl installed on the remote host is prior to 7.87.0. It is therefore affected by a use-after-free vulnerability. Curl can be asked to tunnel virtually all protocols it supports through an HTTP proxy. HTTP proxies can (and often do) deny such tunnel operations. When getting denied to tunnel the specific protocols SMB or TELNET, curl would use a heap-allocated struct after it had been freed, in its transfer shutdown code path. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade Curl to version 7.87.0 or later
https://curl.se/docs/CVE-2022-43552.html

106. Oracle Java SE 1.7.0_301 / 1.8.0_291 / 1.11.0_11 / 1.16.0_1 Multiple Vulnerabilities (Apr 2021 CPU): The remote host is affected by multiple vulnerabilities.

Severity	Medium	Status	Open

First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 301, 8 Update 291, 11 Update 11, or 16 Update 1. It is, therefore, affected by multiple vulnerabilities as referenced in the April 2021 CPU advisory: - A vulnerability in Java SE, SE Embedded and Oracle GraalVM Enterprise Edition allows unauthenticated remote attacker to compromise the system which can result in an unauthorized creation, deletion or modification access to critical data. (CVE-2021-2161) - A vulnerability in Java SE, SE Embedded and Oracle GraalVM Enterprise Edition allows unauthenticated remote attacker with a human interaction from a person other than the attacker to compromise the system which can result in an unauthorized creation, deletion or modification access to critical data. (CVE-2021-2163) 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 April 2021 Oracle Critical Patch Update advisory. https://www.oracle.com/a/tech/docs/cpuapr2021cvrf.xml https://www.oracle.com/security-alerts/cpuapr2021.html#AppendixJAVA

107. SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption): The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.

Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.
https://drownattack.com/ https://drownattack.com/drown-attack-paper.pdf

108. VMware vSphere Client XXE Injection Information Disclosure (VMSA-2016-0022): The remote host has a virtualization client application installed that is affected by an information disclosure vulnerability.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The version of vSphere Client installed on the remote Windows host is affected by an information disclosure vulnerability due to an incorrectly configured XML parser accepting XML external entities (XXE) from an untrusted source. An unauthenticated, remote attacker can exploit this issue to disclose arbitrary files by convincing a user to connect to a malicious instance of a vCenter Server or ESXi host containing specially crafted XML data.

Solution

Upgrade to vSphere Client version 5.5 Update 3e / 6.0 Update 2a or later.
https://www.vmware.com/security/advisories/VMSA-2016-0022.html

109. Potentially Dangerous PATH Variables: Potentially dangerous PATH variables are present in the PATH of the remote host.

Severity	Medium	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

cit-mrtg - (10.10.50.23) - Closed

Description

Potentially dangerous PATH variables are present in the PATH of the remote host, which could lead to privilege escalation by allowing non-administrator users to write files to the PATH directory. This plugin fires on Unix when a directory in the PATH variable is world writable or if '.' (the current directory) is present in the PATH. This plugin also fires when the scan is paranoid and one of the following is true: 1) A directory in the PATH variable is not owned by root 2) A directory in the PATH variable has a group other than root and the group can write to the directory. This plugin fires on Windows when a directory in the PATH variable is writable by one of the following unprivileged identity groups: BUILTIN\Users, NT AUTHORITY\Authenticated Users, anonymous, and everyone. It fires if one of these groups has full, write-only, modify, write owner, generic write, generic all, write data/add file, or write DAC permissions on the PATH directory

Solution

Ensure that directories listed here are in line with corporate policy.

110. ADV180002: Microsoft SQL Server January 2018 Security Update (Meltdown) (Spectre): The remote SQL server is affected by multiple vulnerabilities.

Severity	Medium	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

ReportManager - (10.10.50.71) - Open

- (70.167.3.71) - Open

Description

The remote Microsoft SQL Server is missing a security update. It is, therefore, affected by a vulnerability exists within microprocessors utilizing speculative execution and indirect branch prediction, which may allow an attacker with local user access to disclose information via a side-channel analysis.

Solution

Microsoft has released a set of patches for SQL Server 2008, 2008 R2, 2012, 2014, 2016, and 2017.
http://www.nessus.org/u?573cb1ef http://www.nessus.org/u?6a5c1225
http://www.nessus.org/u?75a275b4 http://www.nessus.org/u?4e0fe7c6
http://www.nessus.org/u?ba131b75 http://www.nessus.org/u?96a526af
http://www.nessus.org/u?f305d4da http://www.nessus.org/u?97d419b3
http://www.nessus.org/u?17660a56 http://www.nessus.org/u?4d20b7cb
http://www.nessus.org/u?df512157 http://www.nessus.org/u?bce5a045
http://www.nessus.org/u?33d23aa9 http://www.nessus.org/u?770a3f93

111. Security Updates for Microsoft .NET core (June 2022): The Microsoft .NET core installations on the remote host are affected by an information disclosure vulnerability.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

An information disclosure vulnerability exists in .NET core 6.0 Less-than 6.0.6 and .NET Core 3.1 Less-than 3.1.26. An unauthenticated, local attacker can exploit this, to disclose potentially sensitive information. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update .NET Core Runtime to version 3.1.26 or 6.0.6.
https://dotnet.microsoft.com/download/dotnet/3.1 https://dotnet.microsoft.com/download/dotnet/6.0 https://github.com/dotnet/announcements/issues/225 http://www.nessus.org/u?bfb8ea98

112. Security Updates for SQL Server Management Studio (August 2020): The SQL Server Management Studio installation on the remote host is missing a security update.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

ReportManager - (10.10.50.71) - Open

- (70.167.3.71) - Open

Description

The SQL Server Management Studio installation on the remote host is missing a security update. It is, therefore, affected by the following vulnerability : - A denial of service vulnerability exists when Microsoft SQL Server Management Studio (SSMS) improperly handles files. An attacker could exploit the vulnerability to trigger a denial of service. (CVE-2020-1455)

Solution

Refer to Microsoft documentation and upgrade to relevant fixed version.

113. Security Update for Microsoft ASP.NET Core (August 2021): The Microsoft ASP.NET Core installations on the remote host is affected by multiple vulnerabilities.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The Microsoft ASP.NET Core installation on the remote host is version 2.1.x prior to 2.1.29, 3.1.x prior to 3.1.18, or 5.x prior to 5.0.9. It is, therefore, affected by multiple vulnerabilities: - A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2021-26423) - An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2021-34485, CVE-2021-34532) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Update ASP.NET Core, remove vulnerable packages and refer to vendor advisory. https://dotnet.microsoft.com/download/dotnet-core/2.1 https://dotnet.microsoft.com/download/dotnet-core/3.1 https://dotnet.microsoft.com/download/dotnet/5.0 https://devblogs.microsoft.com/dotnet/net-august-2021 https://github.com/dotnet/announcements/issues/194 https://github.com/dotnet/announcements/issues/195 https://github.com/dotnet/announcements/issues/196 http://www.nessus.org/u?bb1ce96e http://www.nessus.org/u?0933ffe1 http://www.nessus.org/u?6242d65f

114. SSL Certificate with Wrong Hostname: The SSL certificate for this service is for a different host.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-Azure-VBO - (10.1.1.4) - Open

CIT-SC - (10.10.50.15) - Open

CIT-PWS - (10.10.50.20) - Open

CITS8 - (10.10.50.28) - Open

ReportManager - (10.10.50.71) - Open

cit-android - (10.10.50.115) - Open

NFINIT-VBR - (10.10.102.100) - Open

CIT-TECH - (10.40.50.97) - Open

CIT-PROVISIONING - (10.40.51.12) - Open

- (70.167.3.15) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

- (70.167.3.71) - Open

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

115. SMB Signing not required: Signing is not required on the remote SMB server.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-Azure-VBO - (10.1.1.4) - Open

CIT-SQL - (10.10.50.13) - Open

CIT-ARCH - (10.10.50.14) - Open

CIT-SC - (10.10.50.15) - Open

CIT-PWS - (10.10.50.20) - Open

cIT-RDS - (10.10.50.22) - Open

cit-mrtg - (10.10.50.23) - Open

CIT-MGMT - (10.10.50.25) - Open

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CIT-FS - (10.10.50.30) - Open

CIT-APOLLO - (10.10.50.31) - Open

CIT-ROOT-CA - (10.10.50.32) - Open

CIT-FLEX-HPE - (10.10.50.65) - Open

ReportManager - (10.10.50.71) - Open

LWDC-VEEAM - (10.10.50.102) - Open

cit-android - (10.10.50.115) - Open

CIT-SFTP - (10.10.101.32) - Open

LWDC-PROBE2 - (10.10.101.71) - Open

LWDC-PROBE3 - (10.10.101.72) - Open

NFINIT-UTIL01 - (10.10.101.101) - Open

NFINIT-VBR - (10.10.102.100) - Open

NFINIT-VPROXY3 - (10.10.102.103) - Open

NFINIT-VCLOUD - (10.10.102.110) - Open

CLOUDS1 - (10.20.66.10) - Open

CIT-TECH - (10.40.50.97) - Open

CIT-PROVISIONING - (10.40.51.12) - Open

- (70.167.3.15) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

- (70.167.3.71) - Open

NFINIT-VAC - (10.10.102.112) - Open

NFINIT-VREPO - (10.10.102.111) - Closed

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
http://www.nessus.org/u?df39b8b3 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html http://www.nessus.org/u?a3cac4ea

116. SSL Certificate Expiry: The remote server's SSL certificate has already expired.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target

and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

117. Oracle Java SE 1.7.0_281 / 1.8.0_271 / 1.11.0_9 / 1.15.0_1 Multiple Vulnerabilities (Oct 2020 CPU): The remote host is affected by multiple vulnerabilities

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 281, 8 Update 271, 11 Update 9, or 15 Update 1. It is, therefore, affected by multiple vulnerabilities related to the following components as referenced in the October 2020 CPU advisory: - Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component: Java). Supported versions that are affected are 19.3.3 and 20.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM Enterprise Edition accessible data. (CVE-2020-14803) - Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. (CVE-2020-14792) - Vulnerability in the Java SE, Java

SE Embedded product of Oracle Java SE (component: JNDI). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. (CVE-2020-14781) 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 2020 Oracle Critical Patch Update advisory. https://www.oracle.com/a/tech/docs/cpuoct2020cvrf.xml https://www.oracle.com/security-alerts/cpuoct2020.html

118. Oracle Java SE 1.7.0_291 / 1.8.0_281 / 1.11.0_10 / 1.15.0_2 Information Disclosure (Windows Jan 2021 CPU): The remote host is affected by an information disclosure vulnerability.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 291, 8 Update 281, 11 Update 10, or 15 Update 2. It is, therefore, affected by an information disclosure vulnerability as referenced in the January 2021 CPU advisory. Specifically, an unauthenticated, remote attacker can gain unauthorized read access to some data accessible to Java SE and Java SE Embedded. Only Java deployments that load and run untrusted code and rely on the Java sandbox for security are affected. 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). 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 January 2021 Oracle Critical Patch Update advisory. https://www.oracle.com/a/tech/docs/cpujan2021cvrf.xml https://www.oracle.com/security-alerts/cpujan2021.html#AppendixJAVA

119. Oracle Java SE 1.7.0_331 / 1.8.0_321 / 1.11.0_14 / 1.17.0_2 Multiple Vulnerabilities (January 2022 CPU): The remote host is affected by multiple vulnerabilities.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is affected by multiple vulnerabilities as referenced in the January 2022 CPU advisory: - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21349) - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE,

Oracle GraalVM Enterprise Edition accessible data. Note: 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21291) - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2022-21305) 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 January 2022 Oracle Critical Patch Update advisory. https://www.oracle.com/a/tech/docs/cpujan2022cvrf.xml https://www.oracle.com/security-alerts/cpujan2022.html#AppendixJAVA

120. Oracle Java SE Multiple Vulnerabilities (October 2022 CPU): The remote host is affected by multiple vulnerabilities.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is affected by multiple vulnerabilities as referenced in the October 2022 CPU advisory: - Vulnerability in

the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JGSS). Supported versions that are affected are Oracle Java SE: 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-21618) - VVulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-21624) - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u341, 8u345-perf, 11.0.16.1; Oracle GraalVM Enterprise Edition: 20.3.7, 21.3.3 and 22.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. (CVE-2022-21626) 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 2022 Oracle Critical Patch Update advisory.
https://www.oracle.com/docs/tech/security-alerts/cpuoct2022cvrf.xml
https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixJAVA

121. Oracle Java SE Multiple Vulnerabilities (January 2023 CPU): The remote host is affected by multiple vulnerabilities.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

CITS7 - (10.10.50.27) - Open

LWDC-VEEAM - (10.10.50.102) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is affected by multiple vulnerabilities as referenced in the January 2023 CPU advisory: - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2023-21830) - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. (CVE-2023-21835) - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2023-21843) 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 January 2023 Oracle Critical Patch Update advisory.
https://www.oracle.com/docs/tech/security-alerts/cpujan2023cvrf.xml
https://www.oracle.com/security-alerts/cpujan2023.html#AppendixJAVA

122. Oracle Java SE 1.7.0_231 / 1.8.0_221 / 1.11.0_4 / 1.12.0_2 Multiple Vulnerabilities (Jul 2019 CPU): The remote Windows host contains a programming platform that is affected by multiple vulnerabilities.

Severity	Medium	Status	Open

First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 231, 8 Update 221, 11 Update 4, or 12 Update 2. It is, therefore, affected by multiple vulnerabilities: - Unspecified vulnerabilities in the utilities and JCE subcomponents of Oracle Java SE, which could allow an unauthenticated remote attacker to cause a partial denial of service. (CVE-2019-2762, CVE-2019-2769, CVE-2019-2842) - An unspecified vulnerability in the security subcomponent of Oracle Java SE, which could allow an unauthenticated local attacker to gain unauthorized access to critical Java SE data. (CVE-2019-2745) - Unspecified vulnerabilities in the networking and security subcomponents of Oracle Java SE, which could allow an unauthenticated remote attacker to gain unauthorized access to Java SE data. Exploitation of this vulnerability requires user interaction. (CVE-2019-2766, CVE-2019-2786, CVE-2019-2818) - An unspecified vulnerability in the networking subcomponent of Oracle Java SE, which could allow an unauthenticated remote attacker unauthorized read, update, insert or delete access to Java SE data. (CVE-2019-2816) - An unspecified vulnerability in the JSSE subcomponent of Oracle Java SE, which could allow an unauthenticated, remote attacker to gain unauthorized access to critical Java SE data. Exploitation of this vulnerability requires user interaction. (CVE-2019-2821) - A use after free vulnerability exists in the libpng subcomponent of Oracle Java SE. An unauthenticated, remote attacker can exploit this to cause a complete denial of service condition in Java SE. Exploitation of this vulnerability requires user interaction. (CVE-2019-7317) Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Oracle JDK / JRE 12 Update 2 , 11 Update 4, 8 Update 221 / 7 Update 231 or later. If necessary, remove any affected versions.
http://www.nessus.org/u?9aa2b901

123. SSL Weak Cipher Suites Supported: The remote service supports the use of weak SSL ciphers.

Severity	Medium	Status	Open

First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-TECH - (10.40.50.97) - Open

Description

The remote host supports the use of SSL ciphers that offer weak encryption. Note: This is considerably easier to exploit if the attacker is on the same physical network.

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.
http://www.nessus.org/u?6527892d

124. Terminal Services Doesn't Use Network Level Authentication (NLA) Only: The remote Terminal Services doesn't use Network Level Authentication only.

Severity	Medium	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

cIT-RDS - (10.10.50.22) - Open

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

LWDC-VEEAM - (10.10.50.102) - Open

CLOUDS1 - (10.20.66.10) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

Solution

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) http://www.nessus.org/u?e2628096

125. Oracle Java SE 1.7.x Less-than 1.7.0_211 / 1.8.x Less-than 1.8.0_201 / 1.11.x Less-than 1.11.0_2 Multiple Vulnerabilities (January 2019 CPU): The remote Windows host contains a programming platform that is affected by multiple vulnerabilities.

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

LWDC-VEEAM - (10.10.50.102) - Open

Description

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is prior to 7 Update 211, 8 Update 201, 11 Update 2. It is, therefore, affected by multiple vulnerabilities related to the following components : - An issue in libjpeg 9a, a divide-by-zero error, could allow remote attackers to cause a denial of service condition via a crafted file. (CVE-2018-11212) - An unspecified vulnerability in Oracle Java SE in the Networking subcomponent could allow an unauthenticated, remote attacker with network access via multiple protocols to compromise Java SE. (CVE-2019-2426) - An unspecified vulnerability in Oracle Java SE in the Deployment subcomponent could allow an unauthenticated, remote attacker with network access via multiple protocols to

compromise Java SE. (CVE-2019-2449) - An unspecified vulnerability in Oracle Java SE in the Libraries subcomponent could allow an unauthenticated, remote attacker with network access via multiple protocols to compromise Java SE. (CVE-2019-2422) Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Oracle JDK / JRE 11 Update 2, 8 Update 201 / 7 Update 211 or later. If necessary, remove any affected versions.
http://www.nessus.org/u?799b2d05 http://www.nessus.org/u?c1896887

126. SSH Weak Key Exchange Algorithms Enabled: The remote SSH server is configured to allow weak key exchange algorithms.

Severity	Low	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CIT-SFTP - (10.10.101.32) - Closed

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak. This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes: diffie-hellman-group-exchange-sha1 diffie-hellman-group1-sha1 gss-gex-sha1-* gss-group1-sha1-* gss-group14-sha1-* rsa1024-sha1 Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.
http://www.nessus.org/u?b02d91cd https://datatracker.ietf.org/doc/html/rfc8732

127. VMware Tools 10.x / 11.x / 12.x Less-than 12.1.5 DoS (VMSA-2022-0029): A virtualization tool suite is installed on the remote Windows host is affected by a denial of service vulnerability.

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

NFINIT-UTIL01 - (10.10.101.101) - Open

Description

The version of VMware Tools installed on the remote Windows host is affected by a denial of service vulnerability in the VM3DMP driver. An authenticated, local attacker can exploit this to trigger a PANIC in the VM3DMP driver leading to a denial-of-service condition in the Windows guest OS. 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 VMware Tools version 12.1.5 or later.
https://www.vmware.com/security/advisories/VMSA-2022-0029.html

128. MS15-124: Cumulative Security Update for Internet Explorer (CVE-2015-6161) (3125869): The remote host has a web browser installed that is affected by multiple vulnerabilities.

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The version of Internet Explorer installed on the remote host is missing Cumulative Security Update 3125869 and/or a Registry key to prevent the host against CVE-2015-6161. It is, therefore, affected by Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka 'Microsoft Browser ASLR Bypass'. An unauthenticated, remote attacker can exploit this issue by convincing a user to visit a specially craftedwebsite, resulting in the execution of arbitrary code in the context of the current user. A specific Fix to Run from Microsoft or a registry value must be added to enable the fix for CVE-2015-6161.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10. Refer to KB3125869 for additional information.
http://www.nessus.org/u?f205555e http://www.nessus.org/u?43c16242

129. DNS Server Recursive Query Cache Poisoning Weakness: The remote name server allows recursive queries to be performed by the host running nessusd.

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

- (70.167.3.1) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

Description

It is possible to query the remote name server for third-party names. If this is your internal nameserver, then the attack vector may be limited to employees or guest access if allowed. If you are probing a remote nameserver, then it allows anyone to use it to resolve third party names (such as www.nessus.org). This allows attackers to perform cache poisoning attacks against this nameserver. If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.

Solution

Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN

connected to it). If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf. If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command. Then, within the options block, you can explicitly state: 'allow-recursion { hosts_defined_in_acl }' If you are using another name server, consult its documentation.
http://www.nessus.org/u?c4dcf24a

130. Windows Defender Antimalware/Antivirus Signature Definition Check: Windows Defender AntiMalware / AntiVirus Signatures are continuously not and should not be more than 1 day old

Severity	Low	Status	Open
First Seen on	8th May 2023	Opened On	8th May 2023

Affected Hosts

CIT-MGMT - (10.10.50.25) - Open

Description

Windows Defender has an AntiMalware/AntiVirus signature that gets updated continuously. The signature definition has not been updated in more than 1 day.

Solution

Trigger an update manually and/or enable auto-updates.
https://www.microsoft.com/en-us/wdsi/definitions

131. SSL Certificate Chain Contains RSA Keys Less Than 2048 bits: The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CIT-SQL - (10.10.50.13) - Open

CITS8 - (10.10.50.28) - Open

CIT-FLEX-HPE - (10.10.50.65) - Open

ReportManager - (10.10.50.71) - Open

CIT-TECH - (10.40.50.97) - Open

- (70.167.3.71) - Open

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014. Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.
https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

132. DNS Server Zone Transfer Information Disclosure (AXFR): The remote name server allows zone transfers

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS1 - (10.10.50.21) - Open

CITS4 - (10.10.50.24) - Open

Description

The remote name server allows DNS zone transfers to be performed. A zone transfer lets a remote attacker instantly populate a list of potential targets. In addition, companies often use a naming convention that can give hints as to a servers primary application (for instance, proxy.example.com, payroll.example.com, b2b.example.com, etc.). As such, this information is of great use to an attacker, who may use it to gain information about the topology of the network and spot new targets.

Solution

Limit DNS zone transfers to only the servers that need the information.
https://en.wikipedia.org/wiki/AXFR

133. Microsoft Windows LM / NTLMv1 Authentication Enabled: The remote Windows host is configured to use an insecure authentication protocol.

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS1 - (10.10.50.21) - Open

CITS4 - (10.10.50.24) - Open

Description

The remote host is configured to attempt LM and/or NTLMv1 for outbound authentication. These protocols use weak encryption. A remote attacker who is able to read LM or NTLMv1 challenge and response packets could exploit this to get a user's LM or NTLM hash, which would allow an attacker to authenticate as that user.

Solution

Change the LmCompatibilityLevel setting to 3 or higher.
http://www.nessus.org/u?593e5d9d https://support.microsoft.com/en-us/help/2793313/security-guidance-for-ntlmv1-and-lm-network-authentication http://technet.microsoft.com/en-us/library/cc960646.aspx

134. Terminal Services Encryption Level is not FIPS-140 Compliant: The remote host is

not FIPS-140 compliant.

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CLOUDS1 - (10.20.66.10) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Solution

Change RDP encryption level to : 4. FIPS Compliant

135. Terminal Services Encryption Level is Medium or Low: The remote host is using weak cryptography.

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CLOUDS1 - (10.20.66.10) - Open

CITS7 - WAN - (70.167.3.27) - Open

CIT-CLOUDSYNC-LAN - (70.167.3.50) - Open

CIT-CLOUDSYNC-LAN 1 - (70.167.3.51) - Open

Description

The remote Terminal Services service is not configured to use strong cryptography. Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Solution

Change RDP encryption level to one of : 3. High 4. FIPS Compliant

136. Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities: The remote web server is affected by multiple vulnerabilities.

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS7 - (10.10.50.27) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The 'EBJInvokerServlet' and 'JMXInvokerServlet' servlets hosted on the web server on the remote host are accessible to unauthenticated users. The remote host is, therefore, affected by the following

vulnerabilities : - A security bypass vulnerability exists due to improper restriction of access to the console and web management interfaces. An unauthenticated, remote attacker can exploit this, via direct requests, to bypass authentication and gain administrative access. (CVE-2007-1036) - A remote code execution vulnerability exists due to the JMXInvokerHAServlet and EJBInvokerHAServlet invoker servlets not properly restricting access to profiles. An unauthenticated, remote attacker can exploit this to bypass authentication and invoke MBean methods, resulting in the execution of arbitrary code. (CVE-2012-0874) - A remote code execution vulnerability exists in the EJBInvokerServlet and JMXInvokerServlet servlets due to the ability to post a marshalled object. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to install arbitrary applications. Note that this issue is known to affect McAfee Web Reporter versions prior to or equal to version 5.2.1 as well as Symantec Workspace Streaming version 7.5.0.493 and possibly earlier. (CVE-2013-4810)

Solution

If using EMC Data Protection Advisor, either upgrade to version 6.x or apply the workaround for 5.x. Otherwise, contact the vendor or remove any affected JBoss servlets.

http://www.nessus.org/u?74979c27 https://www.zerodayinitiative.com/advisories/ZDI-13-229/ http://www.nessus.org/u?52567bc1 https://seclists.org/bugtraq/2013/Oct/126 https://www.securityfocus.com/archive/1/530241/30/0/threaded https://seclists.org/bugtraq/2013/Dec/att-133/ESA-2013-094.txt

137. MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483): The remote Windows host is affected by a remote code execution vulnerability.

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS7 - (10.10.50.27) - Open

CITS8 - (10.10.50.28) - Open

CITS7 - WAN - (70.167.3.27) - Open

Description

The remote Windows host is affected by a remote code execution vulnerability due to how the Group

Policy service manages policy data when a domain-joined system connects to a domain controller. An attacker, using a controlled network, can exploit this to gain complete control of the host. Note that Microsoft has no plans to release an update for Windows 2003 even though it is affected by this vulnerability.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.
http://www.nessus.org/u?6533d970 http://www.nessus.org/u?b8230f41

138. MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE): The remote host is affected by a remote information disclosure vulnerability.

Severity	Low	Status	Open
First Seen on	7th April 2023	Opened On	7th April 2023

Affected Hosts

CITS8 - (10.10.50.28) - Open

Description

The remote host is missing one of the workarounds referenced in the Microsoft Security Advisory 3009008. If the client registry key workaround has not been applied, any client software installed on the remote host (including IE) is affected by an information disclosure vulnerability when using SSL 3.0. If the server registry key workaround has not been applied, any server software installed on the remote host (including IIS) is affected by an information disclosure vulnerability when using SSL 3.0. SSL 3.0 uses nondeterministic CBC padding, which allows a man-in-the-middle attacker to decrypt portions of encrypted traffic using a 'padding oracle' attack. This is also known as the 'POODLE' issue.

Solution

Apply the client registry key workaround and the server registry key workaround suggested by Microsoft in the advisory.
https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2015/3009008 https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc http://www.nessus.org/u?f3bc3182 https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-

scsv-00

139. SSH Server CBC Mode Ciphers Enabled: The SSH server is configured to use Cipher Block Chaining.

Severity	Low	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CIT-SFTP - (10.10.101.32) - Closed

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

140. SSH Weak MAC Algorithms Enabled: The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Severity	Low	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CIT-SFTP - (10.10.101.32) - Closed

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

141. SSH Weak Algorithms Supported: The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Severity	Low	Status	Closed
First Seen on	7th April 2023	Closed on	7th April 2023

Affected Hosts

CIT-SFTP - (10.10.101.32) - Closed

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.
https://tools.ietf.org/html/rfc4253#section-6.3