Advisory Alert

Alert Number: AAA20240515 **Date:** May 15, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
FortiGuard	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities
Intel	**High**, Medium, Low	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-17495, CVE-2022-36364, CVE-2024-33006)
Description	SAP has issued monthly security updates addressing multiple vulnerabilities that exist in their products. **CVE-2019-17495** - A Cascading Style Sheets (CSS) injection vulnerability in Swagger UI before 3.23.11 allows attackers to use the Relative Path Overwrite (RPO) technique to perform CSS-based input field value exfiltration, such as exfiltration of a CSRF token value. In other words, this product intentionally allows the embedding of untrusted JSON data from remote servers, but it was not previously known that <style>@import within the JSON data was a functional attack method. **CVE-2022-36364** - Apache Calcite Avatica JDBC driver creates HTTP client instances based on class names provided via `httpclient_impl` connection property; however, the driver does not verify if the class implements the expected interface before instantiating it, which can lead to code execution loaded via arbitrary classes and in rare cases remote code execution. **CVE-2024-33006** - An unauthenticated attacker can upload a malicious file to the server which when accessed by a victim can allow an attacker to completely compromise system. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP Business Client, Versions - 6.5, 7.0, 7.70 SAP Commerce, Version - HY_COM 2205 SAP NetWeaver Application Server ABAP and ABAP Platform, Versions - SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2024.html

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-4761,CVE-2024-30040,CVE-2024-30039,CVE-2024-30038,CVE-2024-30054,CVE-2024-32004,CVE-2024-30051,CVE-2024-30049,CVE-2024-30048,CVE-2024-30045,CVE-2024-30043,CVE-2024-30042,CVE-2024-30041,CVE-2024-30047,CVE-2024-30046,CVE-2024-30037,CVE-2024-30036,CVE-2024-30035,CVE-2024-30034,CVE-2024-30033,CVE-2024-30032,CVE-2024-30031,CVE-2024-30030,CVE-2024-30029,CVE-2024-30028,CVE-2024-30027,CVE-2024-30025,CVE-2024-30024,CVE-2024-29994,CVE-2024-26238,CVE-2024-30059,CVE-2024-30053,CVE-2024-30050,CVE-2024-30044,CVE-2024-30023,CVE-2024-30022,CVE-2024-30021,CVE-2024-30020,CVE-2024-30019,CVE-2024-30018,CVE-2024-30017,CVE-2024-30016,CVE-2024-30015,CVE-2024-30014,CVE-2024-30012,CVE-2024-30011,CVE-2024-30010,CVE-2024-30009,CVE-2024-30008,CVE-2024-30007,CVE-2024-30006,CVE-2024-30005,CVE-2024-30004,CVE-2024-30003,CVE-2024-30002,CVE-2024-30001,CVE-2024-30000,CVE-2024-29999,CVE-2024-29998,CVE-2024-29997,CVE-2024-29996,CVE-2024-32002,CVE-2024-4671,CVE-2024-4559,CVE-2024-4558,CVE-2024-30055,CVE-2024-4368,CVE-2024-4331)
Description	Microsoft has released critical security updates for May 2024. This release includes fixes for several vulnerabilities across various Microsoft products. It is highly recommended that you apply these security patches immediately to protect systems from potential threats.
Affected Products	Microsoft Edge (Chromium-based) - 124.0.2478.105 Windows 10 Version 1607 for 32-bit Systems - 10.0.14393.6981 Windows 10 for x64-based Systems - 10.0.10240.20651 Windows 10 for 32-bit Systems - 10.0.10240.20651 Windows Server 2022, 23H2 Edition (Server Core installation) - 10.0.25398.887 Windows 11 Version 23H2 for x64-based Systems - 10.0.22631.3593 Windows 11 Version 23H2 for ARM64-based Systems - 10.0.22631.3593 Windows 10 Version 22H2 for 32-bit Systems - 10.0.19045.4412 Windows 10 Version 22H2 for ARM64-based Systems - 10.0.19045.4412 Windows 10 Version 22H2 for x64-based Systems - 10.0.19045.4412 Windows 11 Version 22H2 for x64-based Systems - 10.0.22621.3593 Windows 11 Version 22H2 for ARM64-based Systems - 10.0.22621.3593 Windows 10 Version 21H2 for x64-based Systems - 10.0.19044.4412 Windows 10 Version 21H2 for ARM64-based Systems - 10.0.19044.4412 Windows 10 Version 21H2 for 32-bit Systems - 10.0.19044.4412 Windows 11 version 21H2 for ARM64-based Systems - 10.0.22000.2960 Windows 11 version 21H2 for x64-based Systems - 10.0.22000.2960 Windows Server 2022 (Server Core installation) - 10.0.20348.2461 Windows Server 2022 (Server Core installation) - 10.0.20348.2458 Windows Server 2022 - 10.0.20348.2461 Windows Server 2022 - 10.0.20348.2458 Windows Server 2019 (Server Core installation) - 10.0.17763.5820 Windows Server 2019 - 10.0.17763.5820 Windows 10 Version 1809 for ARM64-based Systems - 10.0.17763.5820 Windows 10 Version 1809 for x64-based Systems - 10.0.17763.5820 Windows 10 Version 1809 for 32-bit Systems - 10.0.17763.5820 Windows Server 2012 R2 (Server Core installation) - 6.3.9600.21972 Windows Server 2012 R2 - 6.3.9600.21972 Windows Server 2012 (Server Core installation) - 6.2.9200.24868 Windows Server 2012 - 6.2.9200.24868 Windows Server 2016 (Server Core installation) - 10.0.14393.6981 Windows Server 2016 - 10.0.14393.6981 Windows 10 Version 1607 for x64-based Systems - 10.0.14393.6981 PowerBI-client JS SDK - 2.23.1 Microsoft Visual Studio 2022 version 17.8 - 17.8.10 Microsoft Visual Studio 2022 version 17.6 - 17.6.15 Microsoft Visual Studio 2022 version 17.4 - 17.4.19 Microsoft Visual Studio 2022 version 17.9 - 17.9.7 Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10) - 16.11.36 Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8) - 15.9.62 Dynamics 365 Customer Insights - 1.38813.80 .NET 7.0 7.0.19 .NET 8.0 8.0.5 Microsoft SharePoint Server Subscription Edition - 16.0.17328.20292 Microsoft SharePoint Server 2019 - 16.0.10409.20047 Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for 32-bit editions Office Online Server - 16.0.10410.20003 Microsoft Bing Search for iOS - 28.2.000000000 Microsoft SharePoint Enterprise Server 2016 - 16.0.5448.1000 Microsoft Excel 2016 (64-bit edition) - 16.0.5448.1000 Microsoft Excel 2016 (32-bit edition) - 16.0.5448.1000 Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC for Mac 202116.85.24051214 Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft 365 Apps for Enterprise for 32-bit Systems Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation 6.1.7601.27117 Windows Server 2008 R2 for x64-based Systems Service Pack 1 - 6.1.7601.27117 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) 6.0.6003.22668 Windows Server 2008 for x64-based Systems Service Pack 2 - 6.0.6003.22668 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) - 6.0.6003.22668 Windows Server 2008 for 32-bit Systems Service Pack 2 - 6.0.6003.22668 Microsoft Intune Mobile Application Management for Android - 5.0.6215.0 Azure Migrate - 6.1.294.1008 Microsoft Edge (Chromium-based) - 124.0.2478.97 Microsoft Edge (Chromium-based) - 124.0.2478.80
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-May

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-31466, CVE-2024-31467, CVE-2024-31468, CVE-2024-31469, CVE-2024-31470, CVE-2024-31471, CVE-2024-31472, CVE-2024-31473, CVE-2024-31474, CVE-2024-31475, CVE-2024-31476, CVE-2024-31477, CVE-2024-31478, CVE-2024-31479, CVE-2024-31480, CVE-2024-31481, CVE-2024-31482, CVE-2024-31483)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution, Arbitrary Command Execution, Compromise of System Integrity, Denial of Service, Disclosure of Privileged Information. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ArubaOS 10.5.x.x: 10.5.1.0 and below ArubaOS 10.4.x.x: 10.4.1.0 and below InstantOS 8.11.x.x: 8.11.2.1 and below InstantOS 8.10.x.x: 8.10.0.10 and below InstantOS 8.6.x.x: 8.6.0.23 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04647en_us&docLocale=en_US

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-27504, CVE-2023-28383, CVE-2023-28402, CVE-2023-45733, CVE-2023-45745, CVE-2023-46103, CVE-2023-47252, CVE-2023-47855, CVE-2024-0762, CVE-2024-1598, CVE-2024-25078, CVE-2024-25079, CVE-2024-27353)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution, Denial of Service, Privilege Escalation and Information Disclosure. Lenovo advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-158632

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Use-after-free, null pointer dereference, Denial of service. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.4, 15.5 openSUSE Leap Micro 5.3, 5.4 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise Desktop 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise High Availability Extension 12 SP5, 15 SP3, 15 SP4 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3, LTSS 15 SP4 SUSE Linux Enterprise Live Patching 12 SP5, 15 SP3, 15 SP4 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 12 SP5, 15 SP4 SUSE Linux Enterprise Server 12 SP5, 15 SP3 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux 15-SP3 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5 SUSE Manager Proxy 4.2, 4.3 SUSE Manager Retail Branch Server 4.2, 4.3 SUSE Manager Server 4.2, 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241641-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241642-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241643-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241644-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241645-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241646-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241647-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241648-1

Affected Product	**FortiGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-31488, CVE-2023-45586, CVE-2024-31491, CVE-2024-23107, CVE-2024-23667, CVE-2024-23668, CVE-2024-23669, CVE-2024-23670, CVE-2024-31493, CVE-2024-23664, CVE-2023-36640, CVE-2023-45583, CVE-2023-50180, CVE-2023-46714, CVE-2024-23105, CVE-2023-48789, CVE-2024-21760, CVE-2024-23665)
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Use-after-free, null pointer dereference, Denial of service, Cross site scripting. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiADC 6.2 all versions FortiADC 7.0 all versions FortiADC 7.1 all versions FortiADC 7.2.0 through 7.2.3 FortiADC 7.4.0 through 7.4.1 FortiAuthenticator 6.4 all versions FortiAuthenticator 6.5.0 through 6.5.3 FortiAuthenticator 6.6.0 FortiNAC 7.2.0 through 7.2.3 FortiNAC 8.7 all versions FortiNAC 8.8 all versions FortiNAC 9.1 all versions FortiNAC 9.2 all versions FortiNAC 9.4.0 through 9.4.4 FortiOS 6.0.0 through 6.0.16 FortiOS 6.2 all versions FortiOS 6.4 all versions FortiOS 7.0 all versions FortiOS 7.2.0 through 7.2.7 FortiOS 7.4.0 through 7.4.1 FortiPAM 1.0 all versions FortiPAM 1.1.0 FortiPortal 6.0.0 through 6.0.14 FortiPortal 7.0.0 through 7.0.6 FortiPortal 7.2.0 through 7.2.1 FortiProxy 1.0 all versions FortiProxy 1.1 all versions FortiProxy 1.2 all versions FortiProxy 2.0 all versions FortiProxy 7.0.0 through 7.0.13 FortiProxy 7.2.0 through 7.2.7 FortiProxy 7.4.0 through 7.4.1 FortiSandbox 4.2.0 through 4.2.6 FortiSandbox 4.4.0 through 4.4.4 FortiSOAR 6.4 all versions FortiSOAR 7.0 all versions FortiSOAR 7.2 all versions FortiSOAR 7.3 all versions FortiSOAR 7.4 all versions FortiSwitchManager 7.0.0 through 7.0.2 FortiSwitchManager 7.2.0 through 7.2.2 FortiWeb 6.3 all versions FortiWeb 6.4 all versions FortiWeb 7.0 all versions FortiWeb 7.2.0 through 7.2.7 FortiWeb 7.4.0 through 7.4.2 FortiWebManager 6.0.2 FortiWebManager 6.2.3 through 6.2.4 FortiWebManager 6.3.0 FortiWebManager 7.0.0 through 7.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-23-474 • https://www.fortiguard.com/psirt/FG-IR-24-040 • https://www.fortiguard.com/psirt/FG-IR-23-225 • https://www.fortiguard.com/psirt/FG-IR-24-054 • https://www.fortiguard.com/psirt/FG-IR-23-191 • https://www.fortiguard.com/psirt/FG-IR-23-222 • https://www.fortiguard.com/psirt/FG-IR-24-052 • https://www.fortiguard.com/psirt/FG-IR-23-465 • https://www.fortiguard.com/psirt/FG-IR-23-137 • https://www.fortiguard.com/psirt/FG-IR-23-433 • https://www.fortiguard.com/psirt/FG-IR-23-415 • https://www.fortiguard.com/psirt/FG-IR-24-021 • https://www.fortiguard.com/psirt/FG-IR-23-406 • https://www.fortiguard.com/psirt/FG-IR-23-420 • https://www.fortiguard.com/psirt/FG-IR-23-195

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-29526, CVE-2022-21698, CVE-2021-41190, CVE-2018-20699 CVE-2023-39325, CVE-2023-48795)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause a Memory exhaustion, Denial of Service, Information Disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Fusion - Version(s) 2.3.0 - 2.7.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7151145

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28165, CVE-2024-32730, CVE-2024-34687, CVE-2024-32733 CVE-2024-33002, CVE-2024-32731, CVE-2024-33008, CVE-2024-4139, CVE-2024-4138, CVE-2024-33004, CVE-2024-33009, CVE-2024-33000, CVE-2024-33007)
Description	SAP has issued monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of Service, Sensitive Information Disclosure, Arbitrary Code Execution, Cross-Site Scripting. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP BusinessObjects (Business Intelligence Platform), Versions – 430, 440 SAP Enable Now, Version – 1704 SAP NetWeaver Application server for ABAP and ABAP Platform, Versions - SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 795, SAP_BASIS 796 SAP NetWeaver Application Server ABAP and ABAP Platform, Versions - SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758 SAP S/4HANA (Document Service Handler for DPS), Versions – SAP_BASIS 740, SAP_BASIS 750 My Travel Requests, Version – 600 SAP Process Integration, Versions - MESSAGING 7.31, MESSAGING 7.40, MESSAGING 7.50, NWCEIDE 7.31, SAP_XIESR 7.31, SAP_XIESR 7.40, SAP_XIESR 7.50, SAP_XITOOL 7.31, SAP_XITOOL 7.40, SAP_XITOOL 7.50, SAP_XIAF 7.31, SAP_XIAF 7.40, SAP_XIAF 7.50, SAP_XIGUILIB 7.31, SAP_XIGUILIB 7.40, SAP_XIGUILIB 7.50 SAP Replication Server, Versions – 16.0, 16.0.3, 16.0.4 SAP S/4 HANA (Manage Bank Statement Reprocessing Rules), Versions – SAPSCORE 131, S4CORE 105, S4CORE 106, S4CORE107, S4CORE 108 SAP BusinessObjects Business Intelligence Platform (Webservices), Versions – 430, 440 SAP Process Integration, Versions - MESSAGING 7.10, MESSAGING 7.11, MESSAGING 7.30, MESSAGING 7.31, MESSAGING 7.40, MESSAGING 7.50, NWCEIDE 7.31, SAP_XITOOL 7.00, SAP_XITOOL 7.01, SAP_XITOOL 7.02, SAP_XITOOL 7.10, SAP_XITOOL 7.11, SAP_XITOOL 7.30, SAP_XITOOL 7.31, SAP_XITOOL 7.40, SAP_XITOOL 7.50, SAP_XIAF 7.31, SAP_XIAF 7.40, SAP_XIAF 7.50, SAP_XIPCK 7.00, SAP_XIPCK 7.01, SAP_XIPCK 7.02, SAP_XIPCK 7.10, SAP_XIPCK 7.11, SAP_XIPCK 7.30 SAP Global Label Management (GLM), Versions – 605, 606, 616, 617 SAP Bank Account Management, Versions – 100, 101, 102, 103, 104, 105, 106, 107, 108 SAPUI5, Versions – 754, 755, 756, 757, 758
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2024.html

Affected Product	**Intel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21814,CVE-2024-21828,CVE-2021-33141,CVE-2021-33162,CVE-2021-33157,CVE-2021-33161,CVE-2022-37341,CVE-2021-33145,CVE-2021-33158,CVE-2021-33142,CVE-2021-33146,CVE-2023-42668,CVE-2022-37410,CVE-2024-22015,CVE-2024-22382,CVE-2024-23487,CVE-2024-24981,CVE-2024-23980,CVE-2024-22095,CVE-2023-22662,CVE-2023-49614,CVE-2024-22390,CVE-2023-41092,CVE-2023-28402,CVE-2023-27504,CVE-2023-28383,CVE-2024-21831,CVE-2024-21774,CVE-2023-46103,CVE-2023-45733)
Description	Intel has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Privilege escalation, Denial of service, Information disclosure. Intel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01032.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01056.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00756.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00962.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00916.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00996.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01080.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01050.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01007.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00814.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01069.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01054.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01052.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01051.html

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52628, CVE-2024-25744)
Description	Red Hat has released security updates addressing Multiple Vulnerabilities that exist in their products. **CVE-2023-52628 -** In the Linux kernel, the following vulnerability has been resolved: netfilter: nftables: exthdr: fix 4-byte stack OOB write If priv->len is a multiple of 4, then dst[len / 4] can write past the destination array which leads to stack corruption. This construct is necessary to clean the remainder of the register in case ->len is NOT a multiple of the register size, so make it conditional just like nft_payload.c does. The bug was added in 4.1 cycle and then copied/inherited when tcp/sctp and ip option support was added. Bug reported by Zero Day Initiative project (ZDI-CAN-21950, ZDI-CAN-21951, ZDI-CAN-21961). **CVE-2024-25744 -** A flaw was found in the Linux kernel. A VMM can inject external interrupts on any arbitrary vector at any time, which may allow the guest OS to be manipulated from the VMM side. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:2845 • https://access.redhat.com/errata/RHSA-2024:2846

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.