Advisory Alert

Alert Number: AAA20250312 **Date:** March 12, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Arbitrary Code Execution Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ivanti	**High**	Privilege Escalation Vulnerability
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
FortiGuard	**High**, **Medium**, **Low**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Joomla!	**Low**	Malicious File Upload Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2020-13936)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products **CVE-2020-13936** - Apache Velocity could allow a remote attacker to execute arbitrary code on the system, caused by a sandbox bypass flaw. By modifying the Velocity templates, an attacker could exploit this vulnerability to execute arbitrary code with the same privileges as the account running the Servlet container. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM 7.5 - 7.5.0 UP8 IF03
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7160134

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-26634, CVE-2025-26645, CVE-2025-26633, CVE-2025-24993, CVE-2025-24992, CVE-2025-24983, CVE-2025-24084, CVE-2025-24071, CVE-2025-24067, CVE-2025-24061, CVE-2025-24059, CVE-2025-24055, CVE-2025-24050, CVE-2025-24048, CVE-2025-21247, CVE-2025-24995, CVE-2025-21180, CVE-2025-24083, CVE-2025-24044, CVE-2025-26631, CVE-2025-26630, CVE-2025-26629, CVE-2025-26627, CVE-2025-24049, CVE-2025-24994, CVE-2025-24991, CVE-2025-24985, CVE-2025-24984, CVE-2025-24076, CVE-2025-24075, CVE-2025-24072, CVE-2025-24066, CVE-2025-24064, CVE-2025-24056, CVE-2025-24054, CVE-2025-24051, CVE-2025-24046, CVE-2025-24045, CVE-2025-21199, CVE-2025-25008, CVE-2025-25003, CVE-2025-24998, CVE-2025-24997, CVE-2025-24996, CVE-2025-24988, CVE-2025-24987, CVE-2025-24986, CVE-2025-24082, CVE-2025-24081, CVE-2025-24080, CVE-2025-24079, CVE-2025-24078, CVE-2025-24077, CVE-2025-24070, CVE-2025-24057, CVE-2025-24043, CVE-2024-9157, CVE-2025-24035, CVE-2025-1915, CVE-2025-1914, CVE-2025-1923, CVE-2025-1922, CVE-2025-1921, CVE-2025-1919, CVE-2025-1918, CVE-2025-1917, CVE-2025-1916, CVE-2025-26643, CVE-2025-21253, CVE-2025-21177, CVE-2025-21279, CVE-2025-21267, CVE-2025-21404)
Description	Microsoft has released security updates for the month of March, addressing multiple vulnerabilities that exist in variety of Microsoft products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64 / 32-bit Systems Windows 10 for x64 / 32-bit Systems Windows Server 2025 Windows 11 Version 24H2 for x64 / ARM64-based Systems Windows Server 2022, 23H2 Edition (Server Core installation) Windows 11 Version 23H2 for x64 / ARM64-based Systems Windows Server 2025 (Server Core installation) Windows 10 Version 22H2 for x64 / 32-bit / ARM64-based Systems Windows 11 Version 22H2 for x64 / ARM64-based Systems Windows 10 Version 21H2 for x64 / 32-bit / ARM64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for x64 / 32-bit Systems Windows App Client for Windows Desktop Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Microsoft Office LTSC for Mac 2024 Microsoft Office LTSC 2024 for 64-bit / 32-bit editions Microsoft Office LTSC 2021 for 64-bit / 32-bit editions Microsoft Office LTSC for Mac 2021 Remote Desktop client for Windows Desktop Visual Studio Code Microsoft Access 2016 (64-bit / 32-bit edition) Microsoft 365 Apps for Enterprise for 64-bit / 32-bit Systems Microsoft Office 2019 for 64-bit / 32-bit editions Azure ARC Azure CLI Microsoft Excel 2016 (64-bit / 32-bit edition) Office Online Server Azure Agent for Backup Azure Agent for Site Recovery Microsoft Visual Studio 2022 versions 17.13 / 17.12 / 17.10 / 17.8 Microsoft Visual Studio 2019 versions 16.11 (includes 16.0 - 16.10) Microsoft Visual Studio 2017 versions 15.9 (includes 15.0 - 15.8) Azure promptflow-tools Azure promptflow-core Microsoft Office 2016 (64-bit / 32-bit edition) Microsoft Word 2016 (64-bit / 32-bit edition) ASP.NET Core versions 9.0 / 8.0 WinDbg Microsoft Edge (Chromium-based)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2025-Mar

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52922, CVE-2024-50302, CVE-2024-53197, CVE-2023-52605, CVE-2024-50264, CVE-2024-53113)
Description	Red Hat has released security updates addressing Multiple Vulnerabilities that exist in their products. Exploitation of these vulnerabilities may allow an attacker to cause NULL pointer dereference, out-of-bound access, slab-use-after-free, disclosure of kernel memory. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat Enterprise Linux Server - AUS 8.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:2627 • https://access.redhat.com/errata/RHSA-2025:2646

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may allow an attacker to cause use-after-free, out-of-bound access, memory leak, integer overflow, NULL pointer dereference. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap: 15.5, 15.4 SUSE Linux Enterprise High Performance Computing: 12 SP5, 15 SP4, 15 SP5, ESPOS 15 SP4, 15 SP5, LTSS 15 SP4, 15 SP5 SUSE Linux Enterprise Micro: 5.3, 5.4, 5.5, for Rancher 5.3, 5.4 SUSE Linux Enterprise Server: 12 SP5, 15 SP4, 15 SP5, LTSS, LTSS Extended Security, for SAP Applications 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise Real Time: 15 SP4, 15 SP5 SUSE Linux Enterprise High Availability Extension: 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching: 12-SP5, 15-SP4, 15-SP5 SUSE Manager Versions: Proxy, Retail Branch Server, Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20250833-2/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250577-2/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250201-2/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250835-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250834-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250833-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250835-1/

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2025-22454)
Description	Ivanti has released security updates addressing a Privilege Escalation Vulnerability that exist in their products. **CVE-2025-22454 -** Insufficiently restrictive permissions in Ivanti Secure Access Client before 22.7R4 allows a local authenticated attacker to escalate their privileges. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Secure Access Client (ISAC) 22.7R3 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/March-Security-Advisory-Ivanti-Secure-Access-Client-ISAC-CVE-2025-22454?language=en_US

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36886, CVE-2024-44931, CVE-2024-50117, CVE-2024-35896, CVE-2024-50229, CVE-2024-40981, CVE-2022-48772, CVE-2024-49902,CVE-2024-53164, CVE-2024-41063, CVE-2024-50233, CVE-2024-36952,CVE-2024-43892, CVE-2024-36964, CVE-2024-43900, CVE-2023-52799,CVE-2024-44938, CVE-2024-40910, CVE-2024-26685, CVE-2024-41064,CVE-2024-43863, CVE-2023-52818, CVE-2024-38567, CVE-2024-53156,CVE-2023-52522, CVE-2024-50134, CVE-2024-40911, CVE-2024-40943,CVE-2024-50148, CVE-2024-42068, CVE-2024-53104, CVE-2023-52880,CVE-2024-42070, CVE-2024-38558, CVE-2023-52488, CVE-2024-43893,CVE-2024-50171, CVE-2024-23848)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to use-after-free, NULL pointer dereference, Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 18.04 Ubuntu 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7342-1

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36347, CVE-2023-51385, CVE-2016-3709, CVE-2022-2309, CVE-2016-9318, CVE-2023-4408, CVE-2024-1737, CVE-2024-1975, CVE-2024-7264, CVE-2024-0397, CVE-2024-4032, CVE-2023-27043, CVE-2024-6232, CVE-2024-6923, CVE-2024-7592, CVE-2024-9287, CVE-2024-11168, CVE-2024-45490, CVE-2024-45491, CVE-2024-45492, CVE-2021-20234, CVE-2021-20235, CVE-2021-20237, CVE-2019-19244, CVE-2021-36690, CVE-2023-7104, CVE-2024-21096, CVE-2022-1304, CVE-2020-25659, CVE-2024-52533, CVE-2018-7169, CVE-2023-4641, CVE-2023-29383, CVE-2024-12084, CVE-2024-12085, CVE-2024-12086, CVE-2024-12087, CVE-2024-12088, CVE-2024-12747)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell 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.dell.com/support/kbdoc/en-us/000275716/dsa-2025-052 • https://www.dell.com/support/kbdoc/en-us/000293664/dsa-2025-110-security-update-for-dell-connectrix-fos-and-sanav-vulnerability • https://www.dell.com/support/kbdoc/en-us/000293638/dsa-2025-069-security-update-for-dell-networking-os10-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-11187, CVE-2019-12900, CVE-2025-1094, CVE-2020-11023, CVE-2024-53104, CVE-2025-1244, CVE-2022-49043, CVE-2023-25193, CVE-2023-43804, CVE-2023-45803, CVE-2023-31122, CVE-2023-45802, CVE-2019-11358, CVE-2020-11023, CVE-2020-11022, CVE-2020-23064, CVE-2023-29483, CVE-2023-3635, CVE-2024-33599, CVE-2024-3019, CVE-2023-31484, CVE-2024-25062, CVE-2021-40153, CVE-2021-41072, CVE-2020-15778, CVE-2020-13936, CVE-2022-3287, CVE-2024-26458, CVE-2024-26461)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to denial of service, out of bounds write, command injection, Out-of-bounds Read IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM 7.5 - 7.5.0 UP11 IF02 IBM QRadar SIEM 7.5 - 7.5.0 UP8 IF03
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7185353 • https://www.ibm.com/support/pages/node/7160134

Affected Product	**FortiGuard**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-54026, CVE-2023-37933, CVE-2023-42784, CVE-2024-55594, CVE-2024-3661, CVE-2024-54027, CVE-2024-46663, CVE-2024-52961, CVE-2024-52960, CVE-2024-33501, CVE-2023-48790, CVE-2024-55597, CVE-2024-45328, CVE-2024-55592, CVE-2024-45324, CVE-2024-54018, CVE-2024-32123)
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Cross-site Scripting, sensitive Information disclosure, execute arbitrary code or commands. FortiGuard 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.fortiguard.com/psirt/FG-IR-24-353 • https://www.fortiguard.com/psirt/FG-IR-23-216 • https://www.fortiguard.com/psirt/FG-IR-23-115 • https://www.fortiguard.com/psirt/FG-IR-24-170 • https://www.fortiguard.com/psirt/FG-IR-24-327 • https://www.fortiguard.com/psirt/FG-IR-24-331 • https://www.fortiguard.com/psirt/FG-IR-24-306 • https://www.fortiguard.com/psirt/FG-IR-24-130 • https://www.fortiguard.com/psirt/FG-IR-24-305 • https://www.fortiguard.com/psirt/FG-IR-23-353 • https://www.fortiguard.com/psirt/FG-IR-24-439 • https://www.fortiguard.com/psirt/FG-IR-24-261 • https://www.fortiguard.com/psirt/FG-IR-24-377 • https://www.fortiguard.com/psirt/FG-IR-24-325 • https://www.fortiguard.com/psirt/FG-IR-24-110 • https://www.fortiguard.com/psirt/FG-IR-24-124

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27434, CVE-2025-26661, CVE-2024-38286, CVE-2025-24876, CVE-2024-39592, CVE-2025-26658, CVE-2025-26659, CVE-2025-25242, CVE-2025-25244, CVE-2025-27431, CVE-2025-25245, CVE-2025-23194, CVE-2025-0071, CVE-2025-0062, CVE-2025-27433, CVE-2025-23188, CVE-2025-26660, CVE-2025-26656, CVE-2024-41736, CVE-2025-23185, CVE-2024-38819, CVE-2025-27430, CVE-2025-26655, CVE-2025-27432, CVE-2025-27436)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP Commerce (Swagger UI), Version – COM_CLOUD 2211 • SAP NetWeaver (ABAP Class Builder), 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 914 • SAP Commerce Cloud, Version – HY-COM 2205, COM-CLOUD 2211 • SAP Approuter, Version – 2.6.1 to 16.7.1 • SAP PDCE, Versions – S4CORE 102, 103, S4COREOP 104, 105, 106, 107, 108 • SAP Business One (Service Layer), Version – B1_ON_HANA 10.0, SAP-M-BO 10.0 • SAP NetWeaver Application Server ABAP (applications based on SAP GUI for HTML), Versions – KRNL64UC 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.89, KERNEL 7.93, KERNEL 9.14 • SAP Business Warehouse (Process Chains), Versions – DW4CORE 100, DW4CORE 200, DW4CORE 300, DW4CORE 400, DW4CORE 914, SAP_BW 730, SAP_BW 731, SAP_BW 740, SAP_BW 750 • SAP NetWeaver Application Server Java, Version – AJAX-RUNTIME 7.50 • SAP BusinessObjects Business Intelligence Platform (Web Intelligence), Version – ENTERPRISE 430, 2025 • SAP NetWeaver Enterprise Portal (OBN component), Version – EP-RUNTIME 7.50 • SAP Web Dispatcher and Internet Communication Manager, Versions – KRNL64UC 7.53, WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.89, WEBDISP 7.93, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.89, KERNEL 7.93, KERNEL 9.14 • SAP Fiori apps (Posting Library), Versions – S4CORE 103, 104, 105, 106, 107, 108 • SAP Just In Time, Versions – S4CORE 102, 103, 104, 105, 106, 107, ECC-DIMP 618 • SAP Permit to Work, Versions – UIS4HOP1 800, 900 • SAP Business Objects Business Intelligence Platform, Version – ENTERPRISE 430, 2025, 2027 • SAP Datahub, Versions – HY_COM 2205, HY_DHUB 2205, COM_CLOUD 2211, DHUB_CLOUD 2211 • SAP CRM and SAP S/4HANA (Interaction Center), Versions – S4CRM 100, 200, 204, 205, 206, S4FND 102, 103, 104, 105, 106, 107, 108, S4CEXT 107, 108, BBPCRM 701, 702, 712, 713, 714, WEBCUIF 701, 731, 746, 747, 748, 800, 801 • SAP Electronic Invoicing for Brazil (eDocument Cockpit), Versions – SAP_APPL 617, 618, S4CORE 102, 103, 104, 105, 106, 107, 108
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/march-2025.html

Affected Product	**Joomla!**
Severity	**Low**
Affected Vulnerability	Malicious File Upload Vulnerability (CVE-2024-9287)
Description	Joomla has released security updates addressing a Malicious File Upload Vulnerability in their products. This security flaw is caused by inadequate checks in the Media Manager, allowed users with 'edit' privileges to change the file extension to arbitrary extensions, including .php and other potentially executable extensions. Joomla advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Joomla! CMS versions 4.0.0-4.4.11, 5.1.0-5.2.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/961-20250301-core-malicious-file-uploads-via-media-manager.html

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.