Advisory Alert

Alert Number: **AAA20250213** **Date:** **February 13, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Multiple Time-of-check, Time-of-use (TOCTOU) Race Condition vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Juniper	**Critical**	Authentication Bypass Vulnerability
FortiGuard	**Critical**	Authentication Bypass Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
Palo Alto	**High**, **Medium**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Intel	**High**, **Medium**, **Low**	Multiple Vulnerabilities
SolarWinds	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Drupal	**Medium**	Multiple Vulnerabilities
Synology	**Medium**	Security Update
F5	**Medium**	Arbitrary Command Execution Vulnerability

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38657, CVE-2025-22467, CVE-2024-10644)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products **CVE-2024-38657** - External control of a file name in Ivanti Connect Secure before version 22.7R2.4 and Ivanti Policy Secure before version 22.7R1.3 allows a remote authenticated attacker with admin privileges to write arbitrary files. **CVE-2025-22467** - A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.6 allows a remote authenticated attacker to achieve remote code execution. **CVE-2024-10644** - Code injection in Ivanti Connect Secure before version 22.7R2.4 and Ivanti Policy Secure before version 22.7R1.3 allows a remote authenticated attacker with admin privileges to achieve remote code execution. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Connect Secure (ICS) Versions - 22.7R2.5 and below Ivanti Policy Secure (IPS) Versions - 22.7R1.2 and below Ivanti Secure Access Client (ISAC) Versions - 22.7R4 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs?language=en_US

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Time-of-check, Time-of-use (TOCTOU) Race Condition vulnerabilities (CVE-2024-50379, CVE-2024-56337)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products **CVE-2024-50379** - Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability during JSP compilation in Apache Tomcat permits an RCE on case insensitive file systems when the default servlet is enabled for write (non-default configuration). This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.1, from 10.1.0-M1 through 10.1.33, from 9.0.0.M1 through 9.0.97. Users are recommended to upgrade to version 11.0.2, 10.1.34 or 9.0.98, which fixes the issue. **CVE-2024-56337** - Apache Tomcat has a TOCTOU race condition vulnerability (CVE-2024-56337) affecting versions 9.0.0.M1–9.0.97, 10.1.0-M1–10.1.33, and 11.0.0-M1–11.0.1. This is due to incomplete mitigation of CVE-2024-50379 and impacts users on case-insensitive file systems with the default servlet write enabled. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Unified OSS Console (UOC) - prior to 3.1.13 - UOCCORE HPE Unified OSS Console Software Series - prior to 3.1.13 - UOCAM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04805en_us&docLocale=en_US

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21373, CVE-2025-21212, CVE-2025-21394, CVE-2025-21392, CVE-2025-21377, CVE-2025-21371, CVE-2025-21358, CVE-2025-21347, CVE-2025-21200, CVE-2025-21407, CVE-2025-21418, CVE-2025-21376, CVE-2025-21368, CVE-2025-24042, CVE-2025-21414, CVE-2025-21322, CVE-2025-21254, CVE-2025-21216, CVE-2025-21184, CVE-2025-21181, CVE-2025-21179, CVE-2025-21400, CVE-2025-21397, CVE-2025-21390, CVE-2025-21387, CVE-2025-21386, CVE-2025-21381, CVE-2025-21367, CVE-2025-21359, CVE-2025-21350, CVE-2025-21349, CVE-2025-21337, CVE-2025-21198, CVE-2025-21201, CVE-2025-21190, CVE-2025-21410, CVE-2025-21406, CVE-2025-21208, CVE-2025-21194, CVE-2025-21259, CVE-2025-24039, CVE-2025-24036, CVE-2023-32002, CVE-2025-21420, CVE-2025-21419, CVE-2025-21391, CVE-2025-21183, CVE-2025-21182, CVE-2025-21383, CVE-2025-21379, CVE-2025-21375, CVE-2025-21369, CVE-2025-21352, CVE-2025-21351, CVE-2025-21206, CVE-2025-21188, CVE-2025-0451, CVE-2025-0445, CVE-2025-0444, CVE-2025-21342, CVE-2025-21408, CVE-2025-21283, 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 February, 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 11 Version 22H2 for ARM64-based Systems • Windows 10 Version 21H2 for x64-based Systems • Windows 10 Version 21H2 for ARM64-based Systems • Windows 10 Version 21H2 for 32-bit Systems • Windows Server 2022 (Server Core installation) • Windows Server 2022 • Windows Server 2019 (Server Core installation) • Windows 10 Version 22H2 for ARM64-based Systems • Windows 10 Version 22H2 for x64-based Systems • Windows 11 Version 22H2 for x64-based Systems • Microsoft Office 2019 for 64-bit editions • Microsoft Office 2019 for 32-bit editions • Office Online Server • Microsoft Office 2016 (64-bit edition) • Windows Server 2019 • Windows 10 Version 1809 for x64-based Systems • Windows 10 Version 1809 for 32-bit Systems • Windows Server 2012 R2 (Server Core installation) • Windows Server 2012 R2 • Windows Server 2012 (Server Core installation) • Windows Server 2012 • Windows Server 2016 • Windows 10 Version 1607 for x64-based Systems • Windows 10 Version 1607 for 32-bit Systems • Windows 10 for x64-based Systems • Windows 10 for 32-bit Systems • Windows Server 2025 • Windows 11 Version 24H2 for x64-based Systems • Windows 11 Version 24H2 for ARM64-based Systems • Windows Server 2022, 23H2 Edition (Server Core installation) • Windows 11 Version 23H2 for x64-based Systems • Windows 11 Version 23H2 for ARM64-based Systems • Windows Server 2025 (Server Core installation) • 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 • Windows Server 2016 (Server Core installation) • Windows 10 Version 22H2 for 32-bit Systems • Visual Studio Code - JS Debug Extension • Microsoft PC Manager • Microsoft SharePoint Server Subscription Edition • Microsoft SharePoint Server 2019 • Microsoft SharePoint Enterprise Server 2016 • Microsoft Office LTSC 2024 for 64-bit editions • Microsoft Office LTSC 2024 for 32-bit editions • Microsoft Office LTSC 2021 for 32-bit editions • Microsoft Office LTSC 2021 for 64-bit editions • Microsoft 365 Apps for Enterprise for 64-bit Systems • Microsoft 365 Apps for Enterprise for 32-bit Systems • Microsoft Excel 2016 (64-bit edition) • Microsoft Excel 2016 (32-bit edition) • Microsoft Office LTSC for Mac 2024 • Microsoft Office LTSC for Mac 2021 • Microsoft Office 2016 (32-bit edition) • Microsoft HPC Pack 2016 • Microsoft HPC Pack 2019 • Microsoft Surface Hub • Microsoft Surface Pro 9 ARM • Surface Windows Dev Kit • Microsoft Surface Pro 8 • Microsoft Surface Laptop Go • Microsoft Surface Go 2 • Microsoft Surface Hub 3 • Surface Laptop 3 with Intel Processor • Microsoft Surface Hub 2S • Microsoft Surface Pro 7+ • Surface Laptop 4 with AMD Processor • Microsoft Surface Laptop Go 3 • Microsoft Surface Go 3 • Microsoft Surface Laptop Go 2 • Surface Laptop 4 with Intel Processor • Microsoft Outlook for Android • Visual Studio Code • Microsoft AutoUpdate for Mac • CBL Mariner 2.0 ARM • CBL Mariner 2.0 x64 • Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10) • Microsoft Visual Studio 2022 version 17.12 • Microsoft Visual Studio 2022 version 17.10 • Microsoft Visual Studio 2022 version 17.8 • Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8) • Azure Network Watcher VM Extension • Microsoft Edge (Chromium-based) • Microsoft Edge for iOS • Microsoft Edge for Android • Dynamics 365 Sales
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2025-Feb

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2025-21589)
Description	Juniper has released security updates addressing an authentication bypass vulnerability in their products. If exploited, using an alternate path or channel in Juniper Networks Session Smart Router may allow a network-based attacker to bypass authentication and gain administrative control of the device Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	This issue affects Session Smart Router: • from 5.6.7 before 5.6.17 • from 6.0.8 • from 6.1 before 6.1.12-lts • from 6.2 before 6.2.8-lts • from 6.3 before 6.3.3-r2 This issue affects Session Smart Conductor: • from 5.6.7 before 5.6.17 • from 6.0.8 • from 6.1 before 6.1.12-lts • from 6.2 before 6.2.8-lts • from 6.3 before 6.3.3-r2 This issue affects WAN Assurance Managed Routers: • from 5.6.7 before 5.6.17 • from 6.0.8 • from 6.1 before 6.1.12-lts • from 6.2 before 6.2.8-lts • from 6.3 before 6.3.3-r2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2025-02-Out-of-Cycle-Security-Bulletin-Session-Smart-Router-Session-Smart-Conductor-WAN-Assurance-Router-API-Authentication-Bypass-Vulnerability-CVE-2025-21589?language=en_US

Affected Product	**FortiGuard**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerabilities (CVE-2024-55591, CVE-2025-24472)
Description	FortiGuard has released security updates addressing multiple Authentication Bypass Vulnerabilities that exist in their products. **CVE-2024-55591** - An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 allows a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module. **CVE-2025-24472** - An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS 7.0.0 through 7.0.16 and FortiProxy 7.2.0 through 7.2.12, 7.0.0 through 7.0.19 may allow a remote attacker to gain super-admin privileges via crafted CSF proxy requests. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiOS 7.0 Version - 7.0.0 through 7.0.16 FortiProxy 7.2 Version - 7.2.0 through 7.2.12 FortiProxy 7.0 Version - 7.0.0 through 7.0.19
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-535

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53104, CVE-2024-53113)
Description	Red Hat has released security updates addressing Multiple Vulnerabilities that exist in their products. **CVE-2024-53104 -** A vulnerability in the Linux kernel's USB Video Class (UVC) driver was found, leading to an out-of-bounds write. The issue occurs because the allocated buffer for video frames does not account for all possible formats in a stream. **CVE-2024-53113 -** A NULL pointer dereference issue in the Linux kernel's memory management (mm) subsystem was fixed. The bug occurred in alloc_pages_bulk_noprof() when a task migrated between cpusets, causing concurrent modifications to ac->nodemask. This led to ac.preferred_zoneref->zone being NULL, resulting in a crash. Red Hat 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://access.redhat.com/errata/RHSA-2025:1278 • https://access.redhat.com/errata/RHSA-2025:1280 • https://access.redhat.com/errata/RHSA-2025:1281 • https://access.redhat.com/errata/RHSA-2025:1282 • https://access.redhat.com/errata/RHSA-2025:1291

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45016, CVE-2024-47684, CVE-2022-48912, CVE-2022-48923)
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, NULL pointer diffrence. 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, 15.6 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 12 SP5, 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20250414-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250426-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250476-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250462-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250486-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250487-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250494-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250489-1

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21853, CVE-2024-25565, CVE-2024-22185, CVE-2024-24985, CVE-2023-52340, CVE-2024-42154, CVE-2024-47246, CVE-2024-21925, CVE-2023-20581, CVE-2023-20582, CVE-2023-31342, CVE-2023-31343, CVE-2023-31345, CVE-2024-21924, CVE-2023-20508, CVE-2024-21927, CVE-2024-21935, CVE-2024-21936, CVE-2024-39279, CVE-2024-28047, CVE-2024-36293, CVE-2024-31068, CVE-2024-25571, CVE-2024-37020, CVE-2024-21859, CVE-2024-31155, CVE-2024-24852, CVE-2024-36274, CVE-2024-39813, CVE-2024-39286)
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/000283880/dsa-2025-072-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000283888/dsa-2025-085-security-update-for-dell-amd-based-poweredge-server-and-gpu-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000283897/dsa-2025-041-security-update-for-dell-poweredge-server-for-intel-2025-security-advisories-2025-1-ipu • https://www.dell.com/support/kbdoc/en-us/000283913/dsa-2024-381-security-update-for-dell-poweredge-server-for-intel-2024-security-advisories-2024-4-ipu • https://www.dell.com/support/kbdoc/en-us/000283929/dsa-2025-042-dell-poweredge-server-security-update-for-intel-ethernet-controllers-adapters-and-intel-processor-vulnerabilities

Affected Product	**Palo Alto**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0108, CVE-2025-0109, CVE-2025-0110, CVE-2025-0111, CVE-2025-0112, CVE-2024-1135)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Authentication Bypass, Unauthenticated File Deletion, Command Injection, and Authenticated File Read. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 11.2 Versions Prior to 11.2.4-h4 PAN-OS 11.1 Versions Prior to 11.1.6-h1 PAN-OS 10.2 Versions Prior to 10.2.13-h3 PAN-OS 10.1 Versions Prior to 10.1.14-h9 PAN-OS OpenConfig Plugin Versions Prior to 2.1.2 Cortex XDR Agent 8.6 (None on Windows) Cortex XDR Agent 8.5 Versions Prior to 8.5.1 on Windows Cortex XDR Agent 8.4 All on Windows Cortex XDR Agent 8.3-CE Versions Prior to 8.3.101-CE on Windows Cortex XDR Broker VM Versions Prior to 25.105.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2025-0108 • https://security.paloaltonetworks.com/CVE-2025-0109 • https://security.paloaltonetworks.com/CVE-2025-0110 • https://security.paloaltonetworks.com/CVE-2025-0111 • https://security.paloaltonetworks.com/CVE-2025-0112 • https://security.paloaltonetworks.com/CVE-2024-1135

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22126, CVE-2025-0064, CVE-2025-25243, CVE-2025-24876, CVE-2024-38819, CVE-2025-24868, CVE-2025-24875, CVE-2025-24874, CVE-2025-24867, CVE-2025-24870, CVE-2025-0054, CVE-2025-25241, CVE-2025-23187, CVE-2025-23189, CVE-2025-23193, CVE-2023-24527, CVE-2025-24869, CVE-2025-24872, CVE-2025-23190, CVE-2025-23191)
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 NetWeaver AS Java (User Admin Application), Version – 7.50 • SAP BusinessObjects Business Intelligence platform (Central Management Console), Versions -ENTERPRISE 430, 2025 • SAP Supplier Relationship Management (Master Data Management Catalog), Version - SRM_MDM_CAT 7.52 • Library - @sap/approuter, Version - 2.6.1 to 16.7.1 • SAP Enterprise Project Connection, Version – 3.0 • SAP HANA extended application services, advanced model (User Account and Authentication Services), Version - SAP_EXTENDED_APP_SERVICES 1 • SAP Commerce, Versions – HY_COM 2205, COM_CLOUD 2211 • SAP Commerce (Backoffice), Version – HY_COM 2205, COM_CLOUD 2211 • SAP NetWeaver AS Java (User Admin Application), Version – 7.50 • SAP BusinessObjects Platform (BI Launchpad), Version – ENTERPRISE 430, 2025 • SAP GUI for Windows, Version – BC-FES-GUI 8.00 • SAP Commerce Cloud, Versions – HY_COM 2205, COM_CLOUD 2211 • SAP NetWeaver Application Server Java, Versions – EP-BASIS 7.50, FRAMEWORK-EXT 7.50 • SAP Fiori Apps Reference Library (My Overtime Requests), Version – GBX01HR5 605 • SAP NetWeaver and ABAP Platform (SDCCN), Versions – ST-PI 2008_1_700, ST-PI 2008_1_710, ST-PI 740 • SAP NetWeaver Server ABAP, 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 NetWeaver AS Java for Deploy Service, Version – ENGINEAPI 7.50, SERVERCORE 7.50 • SAP NetWeaver Application Server Java, Version - WD-RUNTIME 7.50 • SAP ABAP Platform (ABAP Build Framework), Versions - 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 NetWeaver and ABAP platform (ST-PI), Version - ST-PI 2008_1_700, ST-PI 2008_1_710, ST-PI 740 • SAP Fiori for SAP ERP, Version - SAP_GWFND 740, 750, 751, 752, 753, 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/february-2025.html

Affected Product	**Intel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Intel has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to denial of service, privilege escalation, 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/default.html

Affected Product	**SolarWinds**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28989, CVE-2024-45718, CVE-2024-52611, CVE-2024-52606, CVE-2024-52612)
Description	SolarWinds has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to sensitive information disclosure, server-side request forgery, cross-site scripting. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Web Help Desk 12.8.4 and all previous versions Kiwi Syslog NG 1.3 and previous versions SolarWinds Platform 2024.4.1 and previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28989 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-45718 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-52611 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-52606 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-52612

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Cross Site Request Forgery and Cross Site Scripting. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal Oauth2 Client Versions Prior to 4.1.3 Drupal 10.x, Prior to Spamspan filter 3.2.1 Drupal Config Split module 8.x-1.x, Prior to Config Split 8.x-1.10 Drupal Config Split module 2.0.x, Prior to Config Split 2.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2025-013 • https://www.drupal.org/sa-contrib-2025-016 • https://www.drupal.org/sa-contrib-2025-017

Affected Product	**Synology**
Severity	**Medium**
Affected Vulnerability	Security Update
Description	Synology has released security updates addressing a vulnerability that exists in Active Backup for Business for DSM. This vulnerability allow remote authenticated users with administrator privileges to read/write/delete specific files. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active Backup for Business for DSM 7.2 Active Backup for Business for DSM 7.1 Active Backup for Business for DSM 6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_25_02

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Arbitrary Command Execution Vulnerability (CVE-2024-9287)
Description	F5 has released security updates addressing an Arbitrary Command Execution Vulnerability that exists in their products. **CVE-2024-9287 -** A vulnerability has been found in the CPython \`venv\` module and CLI where path names provided when creating a virtual environment were not quoted properly, allowing the creator to inject commands into virtual environment "activation" scripts (ie "source venv/bin/activate"). This means that attacker-controlled virtual environments are able to run commands when the virtual environment is activated. Virtual environments which are not created by an attacker or which aren't activated before being used (ie "./venv/bin/python") are not affected. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next SPK Versions - 1.7.0 - 1.9.2 BIG-IP Next CNF Versions - 1.1.0 - 1.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000149756

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.