Advisory Alert

Alert Number: AAA20251119 **Date:** November 19, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Solarwinds	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
SolarWinds	**High**, Medium	Multiple Vulnerabilities
Fortinet	**High**, Medium, Low	Multiple Vulnerabilities
Cisco	Medium	Multiple Vulnerabilities

Description

Affected Product	**Solarwinds**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40547, CVE-2025-40548)
Description	Solarwinds has released security updates addressing multiple vulnerabilities vulnerabilities that exist in SolarWinds Serv-U. **CVE-2025-40547 -** A logic error vulnerability exists in Serv-U which when abused could give a malicious actor with access to admin privileges the ability to execute code. **CVE-2025-40548 -** A missing validation process exists in Serv U when abused, could give a malicious actor with access to admin privileges the ability to execute code. Solarwinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Serv-U 15.5.2.2.102
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40547 • https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40548

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist 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	Dell PowerFlex rack Versions prior to 3.7.8.0, 3.8.3.0 Dell Storage Resource Manager Vapp Versions prior to 5.1.1.1 Dell Storage Monitoring and Reporting Vapp Versions prior to 5.1.1.1 Dell Storage Resource Manager Windows/Linux update Versions prior to 5.1.1.1 Dell Storage Monitoring and Reporting Windows/Linux update Versions prior to 5.1.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000391568/dsa-2025-435-security-update-for-dell-powerflex-rack-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000393543/dsa-2025-360-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-4276, CVE-2025-4277)
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	Dell G15 5535 BIOS Versions prior to 1.15.0 Inspiron 14 5445 BIOS Versions prior to 1.15.0 Inspiron 16 5645 BIOS Versions prior to 1.14.2 Inspiron 14 7445 2-in-1 BIOS Versions prior to 1.15.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000336679/dsa-2025-261

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-26466, CVE-2024-12084, CVE-2024-12085, CVE-2024-12086, CVE-2024-12087, CVE-2024-12088, CVE-2024-12747, CVE-2025-37155, CVE-2025-37156, CVE-2025-37157, CVE-2025-37158, CVE-2025-37159, CVE-2025-37160, CVE-2025-37163)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause access restriction bypass, arbitrary command execution, code execution, denial of service, disclosure of information. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Aruba Airwave Software Aruba CX 10000 Switch Series Aruba CX 4100i Switch Series Aruba CX 6000 Switch Series Aruba CX 6100 Switch Series Aruba CX 6200F Switch Series Aruba CX 6300 Switch Series Aruba CX 6400 Switch Series Aruba CX 8320 Switch Series Aruba CX 8325 Switch Series Aruba CX 8360 Switch Series Aruba CX 8400 Switch Series Aruba CX 9300 Switch Series Aruba AirWave Management Platform
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04888en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04971en_us&docLocale=en_US

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 compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.6 Public Cloud Module 15-SP6 Public Cloud Module 15-SP7 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Linux Enterprise High Performance Computing 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20254123-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254128-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254132-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254135-1/

Affected Product	**SolarWinds**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40545, CVE-2025-40549)
Description	SolarWinds has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-40545 -** SolarWinds Observability Self-Hosted is susceptible to an open redirection vulnerability. The URL is not properly sanitized, and an attacker could manipulate the string to redirect a user to a malicious site. The attack complexity is high, and authentication is required. **CVE-2025-40549 -** A Path Restriction Bypass vulnerability exists in Serv-U that when abused, could give a malicious actor with access to admin privileges the ability to execute code on a directory. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Serv-U 15.5.2.2.102 SolarWinds Observability Self-Hosted 2025.4 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40549 • https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40545

Affected Product	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-58412, CVE-2025-59669, CVE-2025-54821, CVE-2025-58413, CVE-2025-53843, CVE-2025-48839, CVE-2025-58034, CVE-2025-54971, CVE-2025-54660, CVE-2025-46215, CVE-2025-46775, CVE-2025-54972, CVE-2025-46373, CVE-2025-46776, CVE-2025-47761)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause execute unauthorized code or commands, Improper access control, Escalation of privilege, Information disclosure. Fortinet 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-25-736 • https://www.fortiguard.com/psirt/FG-IR-25-843 • https://www.fortiguard.com/psirt/FG-IR-25-545 • https://www.fortiguard.com/psirt/FG-IR-25-632 • https://www.fortiguard.com/psirt/FG-IR-25-358 • https://www.fortiguard.com/psirt/FG-IR-25-225 • https://www.fortiguard.com/psirt/FG-IR-25-513 • https://www.fortiguard.com/psirt/FG-IR-25-686 • https://www.fortiguard.com/psirt/FG-IR-25-844 • https://www.fortiguard.com/psirt/FG-IR-24-501 • https://www.fortiguard.com/psirt/FG-IR-25-259 • https://www.fortiguard.com/psirt/FG-IR-25-634 • https://www.fortiguard.com/psirt/FG-IR-25-125 • https://www.fortiguard.com/psirt/FG-IR-25-251 • https://www.fortiguard.com/psirt/FG-IR-25-112

Affected Product	**Cisco**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20374, CVE-2025-20375, CVE-2025-20376, CVE-2025-20377, CVE-2025-20289, CVE-2025-20303, CVE-2025-20304, CVE-2025-20305)
Description	Cisco 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. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Unified CCX Release Versions prior to - 12.5 SU3, 15.0 Cisco Unified Intelligence Center Versions prior to - 12.6, 15.0 Cisco ISE Release Versions prior to - 3.3 Patch 8, 3.4 Patch 2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cc-mult-vuln-gK4TFXSn • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multiple-vulns-O9BESWJH

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.