Advisory Alert

Alert Number: AAA20250411 **Date:** April 11, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Juniper	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Juniper	**High**, **Medium**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-5535, CVE-2020-36242, CVE-2023-3961, CVE-2024-24790)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in IBM Spectrum Protect Plus. These vulnerabilities could be exploited in libcurl, MongoDB, Python, Samba, OpenSSL and Linux. Vulnerabilities include obtaining sensitive information, causing a denial of service condition, the elevation of privileges, remote execution of arbitrary code and bypassing security restrictions. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Protect Plus 10.1.0 to 10.1.16 Versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7230557

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Juniper has released security updates addressing multiple vulnerabilities in Juniper Networks Junos Space. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Juniper Networks Junos Space versions prior to 24.1R3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2025-04-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-24-1R3-release?language=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 15.4 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro for Rancher 5.4 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Server 15 SP4 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20251195-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251194-1/

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-49200, CVE-2024-11679, CVE-2024-43046, CVE-2024-45549, CVE-2022-23829)
Description	Lenovo has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could allow arbitrary code execution, denial of service, information disclosure, or privilege escalation on affected systems. Lenovo advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Converged HX1310 Appliance x3550 M5 UEFI Firmware Converged HX2310-E Appliance x3550 M5 UEFI Firmware Converged HX3310 Nutanix Appliance x3550 M5 UEFI Firmware Converged HX3310-F Appliance x3550 M5 UEFI Firmware Converged HX3510-G Appliance x3650 M5 UEFI Firmware Converged HX5510 Appliance x3650 M5 UEFI Firmware Converged HX5510-C Appliance x3650 M5 UEFI Firmware Converged HX7510 Appliance x3650 M5 UEFI Firmware
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.lenovo.com/us/en/product_security/LEN-193044 • https://support.lenovo.com/us/en/product_security/LEN-95137

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-6387, CVE-2023-48795)
Description	HPE has released security updates addressing multiple vulnerabilities in the HPE Cray XD670 Server. These vulnerabilities could allow remote access restriction bypass and unauthenticated arbitrary code execution on affected systems. **CVE-2024-6387** – The race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE-2023-48795** - The SSH transport protocol with certain OpenSSH extensions, as implemented in OpenSSH before version 9.6 and other affected products, contains a vulnerability that allows remote attackers to bypass integrity checks. This can result in the omission of packets from the extension negotiation message, potentially causing the client and server to establish a connection with downgraded or disabled security features HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Cray XD670 BMC firmware v1.19 or later
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04848en_us&docLocale=en_US

Affected Product	**Juniper**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Juniper Networks has released security updates addressing multiple vulnerabilities in Junos OS and Junos OS Evolved. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Information Disclosure, Arbitrary code Injection. Juniper Networks 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://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=%40sfcec_community_publish_date_formula__c%20descending&numberOfResults=50&f:ctype=[Security%20Advisories]

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52340, CVE-2024-42154, CVE-2023-6291, CVE-2024-7341, CVE-2023-6841, CVE-2024-52317, CVE-2024-47535, CVE-2023-46120, CVE-2023-6134, CVE-2024-7318, CVE-2024-4629, CVE-2024-7260, CVE-2025-21104, CVE-2025-21104)
Description	Dell has released security updates addressing multiple vulnerabilities in the Dell PowerProtect Data Manager DM5500 Appliance and Dell NetWorker Management Console. These vulnerabilities could be exploited by malicious users to compromise the affected system. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerProtect Data Manager DM5500 Appliance Software Versions prior to 5.19 NetWorker Management Console Versions prior to 19.11.0.4 NetWorker Management Console Version 19.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000306486/dsa-2025-137-security-update-for-dell-powerprotect-data-manager-dm5500-appliance-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000294392/dsa-2025-124-security-update-for-dell-networker-management-console-for-http-host-header-injection-vulnerability

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in IBM Spectrum Protect Plus. These vulnerabilities could be exploited in libcurl, MongoDB, Python, Samba, OpenSSL and Linux. Vulnerabilities include obtaining sensitive information, causing a denial of service condition, the elevation of privileges, remote execution of arbitrary code and bypassing security restrictions. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Protect Plus 10.1.0 to 10.1.16 Versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7230557

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.