Advisory Alert

Alert Number: AAA20240801 **Date:** August 1, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
HPE	**High**	Unauthenticated Remote Code Execution Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**Medium**	Multiple Vulnerabilities
Juniper	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products that in turn affect Dell 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 PowerProtect Cyber Recovery Version 19.16.0.2 and prior Dell PowerProtect Data Manager DM5500 Appliance Version 5.16 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000227419/dsa-2024-293-security-update-for-dell-powerprotect-cyber-recovery-for-multiple-third-party-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227424/dsa-2024-290-security-update-for-dell-powerprotect-data-manager-appliance-dm5500-for-multiple-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-32487, CVE-2024-32002)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-32487** - less could allow a remote attacker to execute arbitrary commands on the system. By using a newline character in the name of a file, an attacker could exploit this vulnerability to execute arbitrary commands on the system. **CVE-2024-32002** - MinGit software which is consumed by Microsoft Visual Studio could allow a remote attacker to execute arbitrary code on the system, caused by a path traversal vulnerability. By persuading a victim to open a specially crafted content, an attacker could exploit this vulnerability to execute arbitrary code on the system. 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 UP9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7162077

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Unauthenticated Remote Code Execution Vulnerability (CVE-2024-6387)
Description	HPE has released security updates addressing an Unauthenticated Remote Code Execution vulnerability that exists in the OpenSSH third-party product that in turn affects HPE products. **CVE-2024-6387** - A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a 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. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking • EdgeConnect SD-WAN Orchestrator ▪ All supported versions running on Rocky Linux 9. See resolution section for remediation. • ArubaOS-CX Switches ▪ 10.14.0006 and below ▪ 10.13.1030 and below ▪ 10.12.1050 and below ▪ 10.11.1070 and below ▪ 10.10.1130 and below ▪ Software Releases prior to ArubaOS-CX version 10.10.xxxx are not affected but are currently End of support (EOS) • Aruba Fabric Composer 7.0.2 and below • HPE Networking Instant On all switches and APs currently running 2.9.1 firmware or below in Cloud mode when the "support token" is activated.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04669en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-24806,CVE-2022-48624,CVE-2024-3651,CVE-2019-25162,CVE-2020-36777,CVE-2021-46934,CVE-2021-47013,CVE-2021-47055,CVE-2021-47118,CVE-2021-47153,CVE-2021-47171,CVE-2021-47185,CVE-2022-48627,CVE-2022-48669,CVE-2023-52439,CVE-2023-52445,CVE-2023-52513,CVE-2023-52520,CVE-2023-52528,CVE-2023-52565,CVE-2023-52578,CVE-2023-52594,CVE-2023-52598,CVE-2023-52606,CVE-2023-52607,CVE-2023-52610,CVE-2024-0340,CVE-2024-23307,CVE-2024-26593,CVE-2024-26603,CVE-2023-52477,CVE-2023-52595,CVE-2024-26610,CVE-2024-26615,CVE-2024-26642,CVE-2024-26643,CVE-2024-26659,CVE-2024-26693,CVE-2024-26694,CVE-2024-26743,CVE-2024-26744,CVE-2024-26779,CVE-2024-26872,CVE-2024-26892,CVE-2024-26897,CVE-2024-26901,CVE-2024-26919,CVE-2024-26933,CVE-2024-26934,CVE-2024-26964,CVE-2024-26973,CVE-2024-26993,CVE-2024-27014,CVE-2024-27048,CVE-2024-27052,CVE-2024-27056,CVE-2024-27059,CVE-2023-6240,CVE-2024-26664,CVE-2024-3652,CVE-2024-2357,CVE-2024-25744,CVE-2024-21094,CVE-2024-21085,CVE-2024-21011,CVE-2023-38264,CVE-2023-2953,CVE-2024-32004,CVE-2024-32020,CVE-2024-32021,CVE-2024-32465,CVE-2018-25091,CVE-2021-33198,CVE-2021-34558,CVE-2022-2879,CVE-2022-2880,CVE-2022-41715,CVE-2023-29409,CVE-2023-39318,CVE-2023-39319,CVE-2023-39321,CVE-2023-39322,CVE-2023-39326,CVE-2023-45287,CVE-2023-45803,CVE-2023-48795,CVE-2024-23650,CVE-2024-24786,CVE-2024-28180,CVE-2023-52425, CVE-2023-1255, CVE-2023-2650)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Server-side request forgery, Arbitrary code execution, Denial of service. 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 UP9 IBM Storage Ceph 6.0, 6.1 IBM Storage Ceph 5.3z1-z3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7162077 • https://www.ibm.com/support/pages/node/7160795

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47194, CVE-2023-52444, CVE-2024-26934, CVE-2024-27020, CVE-2024-25739, CVE-2021-46960, CVE-2024-26882, CVE-2024-36016, CVE-2024-26923, CVE-2024-26840, CVE-2021-46933, CVE-2023-46343, CVE-2024-35978, CVE-2024-26857, CVE-2024-26886, CVE-2024-26884, CVE-2024-26901, CVE-2023-52620, CVE-2023-52752, CVE-2024-24857, CVE-2024-24858, CVE-2023-52436, CVE-2024-35984, CVE-2024-24859, CVE-2023-52449, CVE-2021-46932, CVE-2024-36902, CVE-2022-48619, CVE-2023-52469, CVE-2024-35997, CVE-2024-35982)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 16.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6938-1

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-25948, CVE-2024-25947, CVE-2024-38489, CVE-2024-38490, CVE-2024-38481, CVE-2023-48795)
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 iDRAC Service Module Versions prior to 5.3.0.0 Dell SmartFabric OS10 Versions 10.5.6.x, 10.5.5.x, 10.5.4.x, and 10.5.3.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000227444/dsa-2024-086-security-update-for-dell-idrac-service-module-for-memory-corruption-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227456/dsa-2024-335-security-update-for-dell-os10-third-party-vulnerability

Affected Product	**Juniper**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38545, CVE-2023-38546, CVE-2023-23914, CVE-2023-23915, CVE-2020-8284, CVE-2020-8285, CVE-2020-8286, CVE-2018-1000120, CVE-2018-1000122)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Denial of service, Heap based buffer overflow, Information leakage. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS before • All versions before 21.2R3-S8, 21.4R3-S8, 23.4R1-S1, 23.4R2 • All versions before 21.4R3-S5, 22.2R3-S2, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4R3. • All versions before 21.2R1 Junos OS Evolved • All versions before 21.4R3-S4-EVO. • From 22.1-EVO before 22.1R3-S4-EVO. • From 22.3-EVO before 22.3R3-S1-EVO. • From 22.4-EVO before 22.4R2-S1-EVO.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-cURL-vulnerabilities-resolved?language=en_US

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.