Advisory Alert

Alert Number: **AAA20230511** **Date:** **May 11, 2023**

Document Classification Level **:** Public Circulation Permitted | Public

Information Classification Level **:** TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Palo Alto	**Medium**	Multiple Vulnerabilities
HP	**Medium**	Information Disclosure Vulnerability
IBM	**Medium**	XML External Entity (XXE) Injection vulnerability

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1670, CVE-2023-1855, CVE-2023-1989, CVE-2023-1990, CVE-2023-1998, CVE-2023-2124, CVE-2023-2162, CVE-2023-30772, CVE-2020-36691, CVE-2022-43945 , CVE-2023-1611, CVE-2023-2483)
Description	SUSE has released a security update addressing multiple vulnerabilities in their products. If exploited these vulnerabilities could cause use after free condition, out of bound memory access, create a race condition, and buffer overflow. SUSE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Real Time 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232162-1/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26356, CVE-2021-26371, CVE-2021-26406, CVE-2021-46756, CVE-2023-20520, CVE-2021-46769, CVE-2021-26354, CVE-2021-26379, CVE-2021-46763, CVE-2021-46764, CVE-2021-26406 , CVE-2021-46775, CVE-2023-20524, CVE-2021-46762, CVE-2022-23818, CVE-2021-26397)
Description	Dell has released a security update addressing multiple vulnerabilities in their Dell PowerEdge servers that associated with AMD server vulnerabilities. A malicious attacker can use this vulnerabilities to compromise the system. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	PowerEdge R6415 Versions prior to 1.19.0 PowerEdge R7415 Versions prior to 1.19.0 PowerEdge R7425 Versions prior to 1.19.0 PowerEdge XE8545 Versions prior to 2.9.4 PowerEdge C6525 Versions prior to 2.9.4 PowerEdge R6515 Versions prior to 2.9.3 PowerEdge R7515 Versions prior to 2.9.3 PowerEdge R6525 Versions prior to 2.9.3 PowerEdge R7525 Versions prior to 2.9.3 Dell EMC XC Core XC7525 Versions prior to 2.9.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000213267/dsa-2023-105-security-update-for-dell-poweredge-server-for-amd-server-vulnerabilities

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1829, CVE-2023-1872, CVE-2023-1859, CVE-2022-40307, CVE-2023-26545, CVE-2022-3586, CVE-2023-0386, CVE-2022-3303, CVE-2023-0468, CVE-2022-4662, CVE-2023-23455, CVE-2022-2590, CVE-2022-4095)
Description	Ubuntu has released a security update addressing multiple vulnerabilities that exists in the Linux kernel. Successful exploitation of these vulnerabilities could cause privilege escalation, denial of service, arbitrary code execution, and sensitive information disclosure. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6070-1 https://ubuntu.com/security/notices/USN-6071-1 https://ubuntu.com/security/notices/USN-6072-1 https://ubuntu.com/security/notices/USN-6069-1

Affected Product	**Palo Alto**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0007, CVE-2023-0008)
Description	Palo Alto has released security updates addressing multiple vulnerabilities exists in their PAN-OS and Panorama web interfaces. **CVE-2023-0007 -** A cross-site scripting (XSS) vulnerability that exists in Palo Alto Networks PAN-OS software on Panorama appliances. This vulnerability enables an authenticated read-write administrator to store a JavaScript payload in the web interface that will execute in the context of another administrator's browser when viewed. **CVE-2023-0008 -** A file disclosure vulnerability that exists in Palo Alto Networks PAN-OS software. This vulnerability enables an authenticated administrator with access to the web interface to export local files from the firewall through a race condition. Palo Alto recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	PAN-OS 11.0 versions prior to 11.0.1 PAN-OS 10.2 versions prior to 10.2.4 PAN-OS 10.1 versions prior to 10.1.10 PAN-OS 10.0 versions prior to 10.0.12 PAN-OS 9.1 versions prior to 9.1.16 PAN-OS 9.0 versions prior to 9.0.17 PAN-OS 8.1 versions prior to 8.1.25 PAN-OS 10.0 on panorama versions prior to 10.0.7 PAN-OS 9.1 on panorama versions prior to 9.1.16 PAN-OS 9.0 on panorama versions prior to 9.0.17 PAN-OS 8.1 on panorama versions prior to 8.1.25
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2023-0007 https://security.paloaltonetworks.com/CVE-2023-0008

Affected Product	**HP**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2022-38087)
Description	HP has released security updates addressing an Information Disclosure vulnerability that exists in certain HPE servers. **CVE-2022-38087 –** An Information Disclosure Vulnerability that exists on certain HPE servers that can be locally exploited. HP recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE ProLiant BL460c Gen10 Server Blade - Prior to v2.80_04-20-2023 HPE Synergy 480 Gen10 Compute Module - Prior to v2.80_04-20-2023 HPE Synergy 660 Gen10 Compute Module - Prior to v2.80_04-20-2023 HPE Apollo 2000 System - Prior to v2.80_04-20-2023 HPE Apollo 4200 Gen10 Server - Prior to v2.80_04-20-2023 HPE Apollo 4510 Gen10 System - Prior to v2.80_04-20-2023 HPE Apollo 6500 Gen10 System - Prior to v2.80_04-20-2023 HPE ProLiant XL170r Gen10 Server - Prior to v2.80_04-20-2023 HPE ProLiant XL190r Gen10 Server - Prior to v2.80_04-20-2023 HPE ProLiant XL230k Gen10 Server - Prior to v2.80_04-20-2023 HPE ProLiant XL270d Gen10 Server - Prior to v2.80_04-20-2023 HPE ProLiant XL450 Gen10 Server - Prior to v2.80_04-20-2023 HPE ProLiant DX170r Gen10 server - Prior to v2.80_04-20-2023 HPE ProLiant DX190r Gen10 server - Prior to v2.80_04-20-2023 HPE ProLiant DX360 Gen10 server - Prior to v2.80_04-20-2023 HPE ProLiant DX380 Gen10 server - Prior to v2.80_04-20-2023 HPE ProLiant DX560 Gen10 server - Prior to v2.80_04-20-2023 HPE ProLiant DX4200 Gen10 server - Prior to v2.80_04-20-2023
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04477en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04478en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04476en_us

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	XML External Entity (XXE) Injection vulnerability (CVE-2023-27554)
Description	IBM has released a security update addressing an XML External Entity (XXE) Injection vulnerability that exists in WebSphere Application Server. **CVE-2023-27554 –** A XML External Entity Injection Vulnerability that exists in IBM WebSphere Application Server when processing data. A remote attacker can exploit this vulnerability to expose sensitive information or consume memory resources. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM WebSphere Application Server 8.5 and 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6989451

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.