Advisory Alert

Alert Number: AAA20230209 **Date:** February 9, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
IBM	**High , Medium**	Multiple Vulnerabilities
Paloalto	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-0060, CVE-2021-0092, CVE-2022-21123, CVE-2022-21127)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their third party components Intel SPS, Intel BIOS firmware and microcode. If exploited, these vulnerabilities could lead to privilege escalation, denial of service and information disclosure. Dell highly recommends to apply necessary fixes to avoid issues.
Affected Products	Dell EMC Networking VEP1425/VEP1445/VEP1485, Before 3.48.0.9-17 Dell PowerSwitch N2200-ON Series Before N2200-3.45.0.9-10, N3200-ON Series Before N3200-3.45.0.9-7 Dell PowerSwitch S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON Before 3.40.0.9-14 Dell PowerSwitch S5448F-ON Before 3.52.0.D-10, Z9264F-ON Before 3.42.0.9-17 , Z9432F-ON Before 3.51.0.D-11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000208394/dsa-2023-061-dell-emc-networking-bios-security-update-for-multiple-vulnerabilities

Affected Product	**IBM**
Severity	**High , Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-46364, CVE-2022-45787)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to sensitive information disclosure and server-side request forgery. **CVE-2022-46364 -** A server-side request forgery vulnerability was found in Apache CXF, caused by a flaw in parsing the href attribute of XOP:Include in MTOM requests. By using a specially-crafted request, an attacker could exploit this vulnerability to conduct SSRF attack. **CVE-2022-45787 -** A sensitive information disclosure vulnerability was found in Apache James MIME4J, a local authenticated attacker can obtain sensitive information by sending a specially-crafted request to the temporary files which has improper laxist permissions. IBM recommends to apply necessary fixes to avoid issues.
Affected Products	IBM WebSphere Application Server Liberty 17.0.0.3 - 23.0.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6953779 https://www.ibm.com/support/pages/node/6953767

Affected Product	**Paloalto**
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-0001, CVE-2023-0002, CVE-2023-0003)
Description	Paloalto has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to command execution and information disclosure. **CVE-2023-0001-** A vulnerability was found in Palo Alto Networks Cortex XDR agent on Windows devices, a local system administrator allows to disclose the admin password for the agent in cleartext, which bad actors can then use to execute privileged cytool commands that disable or uninstall the agent. **CVE-2023-0002-** A vulnerability was found in protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local user to execute privileged cytool commands that disable or uninstall the agent. **CVE-2023-0003-** A vulnerability was found in the Palo Alto Networks Cortex XSOAR server software enables an authenticated user with access to the web interface to read local files from the server. Paloalto recommends to apply necessary fixes to avoid issues.
Affected Products	Cortex XDR Agent version before 7.5.101-CE on Windows Cortex XDR Agent version before 5.0.12.22203 on Windows Cortex XSOAR 6.10.0, version before 6.10.0.185964 Cortex XSOAR 6.9 version before 6.9.B185415 Cortex XSOAR 6.8 version before 6.8.B185719 Cortex XSOAR 6.6 version before 6.6.B186115
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2023-0001 https://security.paloaltonetworks.com/CVE-2023-0002 https://security.paloaltonetworks.com/CVE-2023-0003

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.