Advisory Alert

Alert Number: **AAA20240415** **Date:** **April 15, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Palo Alto	**Critical**	Command Injection Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
HPE	**High**	Remote Authentication Bypass Vulnerability
Suse	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**Medium**	Denial of Service Vulnerability
PHP	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Palo Alto**
Severity	**Critical**
Affected Vulnerability	Command Injection Vulnerability (CVE-2024-3400)
Description	Palo Alto has released security updates addressing a Command Injection Vulnerability that exists in the GlobalProtect feature of Palo Alto Networks PAN-OS software. If exploited it may allow an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS versions prior to 11.1.2-h3 PAN-OS versions prior to 11.0.4-h1 PAN-OS versions prior to 10.2.9-h1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-3400

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. Malicious users could exploit these vulnerabilities to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Storage Resource Manager- Vapp Versions prior to 5.0.0.0 Dell Storage Monitoring and Reporting- Vapp Versions prior to 5.0.0.0 Dell Storage Resource Manager- Windows/Linux update Versions prior to 5.0.0.0 Dell Storage Monitoring and Reporting- Windows/Linux update Versions prior to 5.0.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000224070/dsa-2024-143-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51385, CVE-2023-42282)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-51385** - OpenSSH could allow a remote attacker to execute arbitrary commands on the system, caused by improper validation of shell metacharacters. By sending a specially crafted request using expansion tokens, an attacker could exploit this vulnerability to execute arbitrary commands on the system. **CVE-2023-42282** - Node.js IP package could allow a remote attacker to execute arbitrary code on the system, caused by a server-side request forgery flaw in the ip.isPublic() function. By sending a specially crafted request using a hexadecimal representation of a private IP address, an attacker could exploit this vulnerability to execute arbitrary code on the system and obtain sensitive information. 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 UP8 IBM Security QRadar Analyst Workflow 1.0.0 - 2.32.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7148190 • https://www.ibm.com/support/pages/node/7148094

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Remote Authentication Bypass Vulnerability (CVE-2024-22439)
Description	HPE has released a security update addressing a Remote Authentication Bypass Vulnerability in HPE FlexFabric and FlexNetwork Switchs. This vulnerability could be exploited to gain privileged access to switches resulting in information disclosure. HPE recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE FlexFabric 5710 Switch Series - Prior to v7.10.R6710 HPE FlexFabric 5940 Switch Series - Prior to v7.10.R6710 HPE FlexFabric 5944 Switch Series - Prior to v7.10.R6710 HPE FlexFabric 5945 Switch Series - Prior to v7.10.R6710 HPE FlexFabric 12900E Switch Series - Prior to v9.10.R5210 HPE FlexNetwork 5130 EI Switch Series - Prior to v7.10.R3507P18 HPE FlexNetwork 5130 HI Switch Series - Prior to v7.10.R3507P10 HPE FlexNetwork 5510 HI Switch Series - Prior to v7.10.R3507P10 HPE FlexNetwork 10500 Switch Series - Prior to v7.10.R7639P01 HPE FLexNetwork MSR95x Router Series - Prior to v7.10.R6728P25 HPE FlexNetwork MSR1000 Router Series - Prior to v7.10.R6728P25 HPE FlexNetwork MSR2000 Router Series - Prior to v7.10.R6728P25 HPE FlexNetwork MSR3000 Router Series - Prior to v7.10.R6728P25 HPE FlexNetwork MSR4000 Router Series - Prior to v7.10.R6728P25
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04625en_us

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52340, CVE-2023-1829, CVE-2023-6531, CVE-2023-1829, CVE-2023-52340, CVE-2024-0565, CVE-2024-1085)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Out-of-bounds memory read, Use-after-free condition and Denial of Service. Suse advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.5 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP2, 15 SP3, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15 SP2, 15 SP3, 15 SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5, 15 SP2, 15 SP3, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP2, 15 SP3, 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241278-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241276-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241275-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241274-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241273-1/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34967, CVE-2023-48795, CVE-2023-39615, CVE-2021-35937, CVE-2021-35938, CVE-2021-35939, CVE-2023-42669, CVE-2023-28322, CVE-2023-46218, CVE-2023-38546, CVE-2023-43804, CVE-2023-45803, CVE-2023-5388, CVE-2023-6135, CVE-2011-4969, CVE-2020-7656, CVE-2015-9251, CVE-2012-6708, CVE-2019-13224, CVE-2019-16163, CVE-2019-19012, CVE-2019-19203, CVE-2019-19204, CVE-2023-26604, CVE-2023-20569, CVE-2022-46329, CVE-2021-41043, CVE-2023-34968, CVE-2023-34966, CVE-2022-2127, CVE-2023-28486, CVE-2023-28487, CVE-2023-42465, CVE-2023-1786, CVE-2020-28241, CVE-2023-22081, CVE-2023-22067, CVE-2023-5676,CVE-2023-27043,CVE-2022-48564, CVE-2022-48560,CVE-2023-2828,CVE-2023-3341,CVE-2022-3094,CVE-2022-45061, CVE-2024-0553, CVE-2023-4091, CVE-2023-44270, CVE-2024-28849, CVE-2023-26159, CVE-2022-26377)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Attackers could exploit these vulnerabilities to cause Heap-based buffer overflow, HTTP request smuggling, Privilege escalation, Sensitive Information disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar Analyst Workflow 1.0.0 - 2.32.0 IBM QRadar SIEM 7.5 - 7.5.0 UP8, UP7 IF06
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7148190 • https://www.ibm.com/support/pages/node/7148094 • https://www.ibm.com/support/pages/node/7145265

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-20294)
Description	Dell has released security updates addressing a Denial of Service Vulnerability that exists in NX-OS SW and MDS 9000 Switches. This vulnerability 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	Products running on NX-OS versions prior to 9.4(1a), including • MDS-9220i • MDS-9250i • MDS-9148S • MDS-9396S • MDS-9148V • MDS-9396T • MDS-9124V • MDS-9148T • MDS-9132T • MDS-9396V • MDS-9718-V3 • MDS-9710-V2 • MDS-9706-V2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000224066/dsa-2024-154-security-update-for-dell-connectrix-nx-os-sw-and-mds-9000-switches-link-layer-discovery-protocol-lldp-vulnerabilities

Affected Product	**PHP**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-2757, CVE-2024-3096, CVE-2024-2756, CVE-2022-31629, CVE-2024-1874)
Description	PHP has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Cookie bypass and Command injection. PHP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PHP versions prior to 8.3.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/ChangeLog-8.php#8.3.6

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.