TLP: WHITE

Advisory Alert

Alert Number: **AAA20240815** **Date:** **August 15, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SolarWinds	**Critical**	Java Deserialization Remote Code Execution vulnerability
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
F5	**High**, **Medium**	Multiple Vulnerabilities
Palo Alto Networks	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Cisco	**Medium**	Content Encoding Filter Bypass Vulnerability
Nginx	**Low**	Buffer Over-read Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-48795, CVE-2023-29499, CVE-2024-25943, CVE-2024-38433, CVE-2022-44640, CVE-2022-34435, CVE-2024-6387, CVE-2022-2309, CVE-2018-18074, CVE-2018-20060, CVE-2019-9740, CVE-2019-11324, CVE-2020-26116)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000227304/dsa-2024-314-security-update-for-dell-powerprotect-dd-idrac9-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000222010/dsa-2024-042-dell-unity-dell-unity-vsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities

Affected Product	**SolarWinds**
Severity	**Critical**
Affected Vulnerability	Java Deserialization Remote Code Execution vulnerability (CVE-2024-28986)
Description	SolarWinds has released security updates addressing a Java Deserialization Remote Code Execution vulnerability that exists in their products. **CVE-2024-28986** - SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. While it was reported as an unauthenticated vulnerability, SolarWinds has been unable to reproduce it without authentication after thorough testing. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Web Help Desk 12.8.3 and all previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28986

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, memory corruption, use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
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 Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro for Rancher 5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242902-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242901-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242911-1/

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-6387, CVE-2024-25079, CVE-2024-27353, CVE-2022-23829, CVE-2023-20593, CVE-2024-0160)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000227795/dsa-2024-342-security-update-for-dell-idrac9-openssh-vulnerability • https://www.dell.com/support/kbdoc/en-us/000226609/dsa-2024-301 • https://www.dell.com/support/kbdoc/en-us/000226608/dsa-2024-300 • https://www.dell.com/support/kbdoc/en-us/000212980/dsa-2024-029-security-update-for-an-amd-bios-vulnerability • https://www.dell.com/support/kbdoc/en-us/000216151/dsa-2024-027-security-update-for-dell-client-platform-amd-bios-vulnerability • https://www.dell.com/support/kbdoc/en-us/000224763/dsa-2024-122-security-update-for-dell-client-bios-for-an-incorrect-authorization-vulnerability

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-37891, CVE-2024-39809, CVE-2024-37028, CVE-2024-41164, CVE-2024-41719, CVE-2024-41727, CVE-2024-39778, CVE-2024-41723)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Information Disclosure. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) versions 17.1.0 - 17.1.1, 16.1.0 - 16.1.5, 15.1.0 - 15.1.10 BIG-IP Next Central Manager versions 20.1.0 - 20.2.0 BIG-IP Next SPK versions 1.7.0 - 1.8.2 BIG-IP Next CNF versions 1.1.0 - 1.1.1 BIG-IQ Centralized Management versions 8.2.0 - 8.3.0 F5OS-A versions 1.7.0, 1.5.1 - 1.5.2 F5OS-C versions 1.6.0 - 1.6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000140711 • https://my.f5.com/manage/s/article/K000140111 • https://my.f5.com/manage/s/article/K000139938 • https://my.f5.com/manage/s/article/K000138477 • https://my.f5.com/manage/s/article/K000140006 • https://my.f5.com/manage/s/article/K000138833 • https://my.f5.com/manage/s/article/K05710614 • https://my.f5.com/manage/s/article/K10438187

Affected Product	**Palo Alto Networks**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-6772, CVE-2024-6773, CVE-2024-6774, CVE-2024-6775, CVE-2024-6776, CVE-2024-6777, CVE-2024-6778, CVE-2024-6779, CVE-2024-6988, CVE-2024-6989, CVE-2024-6990, CVE-2024-6991, CVE-2024-6994, CVE-2024-6995, CVE-2024-6996, CVE-2024-6997, CVE-2024-6998, CVE-2024-6999, CVE-2024-7000, CVE-2024-7001, CVE-2024-7003, CVE-2024-7004, CVE-2024-7005, CVE-2024-7255, CVE-2024-7256, CVE-2024-7532, CVE-2024-7533, CVE-2024-7534, CVE-2024-7535, CVE-2024-7536, CVE-2024-7550, CVE-2024-5914, CVE-2024-5916, CVE-2024-5915)
Description	Palo Alto Networks has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Local Privilege Escalation, Information Disclosure, Command Injection. Palo Alto Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	GlobalProtect App 6.3 versions prior to 6.3.1 on Windows GlobalProtect App 6.2 versions prior to 6.2.4 on Windows GlobalProtect App 6.1 versions prior to 6.1.5 on Windows GlobalProtect App 6.0 versions prior to 6.0.x on Windows GlobalProtect App 5.1 versions prior to 5.1.x on Windows PAN-OS 11.0 versions prior to 11.0.4 PAN-OS 10.2 versions prior to 10.2.8 Cloud NGFW Before 8/15 on Azure, Before 8/23 on AWS Cortex XSOAR CommonScripts versions prior to 1.12.33 Prisma Access Browser versions prior to 126.183.2844.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2024-5915 • https://security.paloaltonetworks.com/CVE-2024-5916 • https://security.paloaltonetworks.com/CVE-2024-5914 • https://security.paloaltonetworks.com/PAN-SA-2024-0007

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6949-2

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Content Encoding Filter Bypass Vulnerability (CVE-2023-20215)
Description	Cisco has released security updates addressing a Content Encoding Filter Bypass Vulnerability that exists in Cisco Secure Web Appliance. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco AsyncOS for Secure Web Appliance Software • Release 14.5 - versions prior to 14.5.3-033 • Release 15.2 - versions prior to 15.2.0-164 • Versions 14.0 and earlier • Version 15.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj

Affected Product	**Nginx**
Severity	**Low**
Affected Vulnerability	Buffer Over-read Vulnerability (CVE-2024-7347)
Description	Nginx has released security updates addressing a Buffer Over-read Vulnerability that exists in their products. **CVE-2024-7347** - NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_mp4_module, which might allow an attacker to over-read NGINX worker memory resulting in its termination, using a specially crafted mp4 file. The issue only affects NGINX if it is built with the ngx_http_mp4_module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger the processing of a specially crafted mp4 file with the ngx_http_mp4_module. Nginx advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Nginx versions 1.5.13-1.27.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://mailman.nginx.org/pipermail/nginx-announce/2024/UUOCLLONPR6244YQYU65PO5LB7JDYCWM.html

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.