Advisory Alert

Alert Number: **AAA20231215** **Date:** **December 15, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Palo Alto	**High ,** **Medium**	Multiple Vulnerabilities
CPanel	**Medium**	Multiple Vulnerabilities
HPE	**Medium,** **Low**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46604)
Description	HPE has released security updates addressing security vulnerabilities identified in HPE Intelligent Management Center. These vulnerabilities could be remotely exploited to allow code execution, unauthorized data access and denial of service. It is highly recommended to apply necessary security fixes at earliest to avoid issues
Affected Products	HPE Intelligent Management Center (iMC) - Prior to 7.3 E0710H02
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04574en_us

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44286, CVE-2023-48668, CVE-2023-44285, CVE-2023-44277, CVE-2023-48667, CVE-2023-44279, CVE-2023-44278, CVE-2023-44284, CVE-2022-36392, CVE-2022-38102, CVE-2022-29871, CVE-2022-44611, CVE-2022-27879, CVE-2022-43505, CVE-2022-40982)
Description	Dell has released security updates addressing multiple security vulnerabilities. These vulnerabilities could be exploited by malicious actors to execute arbitrary commands, gain unauthorized access, perform SQL injection, and compromise system integrity. It is recommended to apply necessary security fixes at earliest to avoid issues
Affected Products	Dell Power Protect DD series appliances 7.0 to 7.12.0.0 Dell Power Protect DD Virtual Edition 7.0 to 7.12.0.0 Dell APEX Protection Storage 7.0 to 7.12.0.0 Power Protect DD Management Center 6.2.1.100 and below, 7.0 to 7.12.0.0 Power Protect DP Series Appliance (IDPA) All Models 2.7.4 and below Power Protect Data Manager Appliance model DM5500 5.14 and below Dell Power Protect DD series appliances and Dell Power Protect DD Virtual Edition leveraged in the Disk Library for Mainframe (DLm) environment 6.2.1.100 and below, 7.0 to 7.12.0.0 Multiple Versions of Inspiron, Alienware Area, Alienware Aurora, Dell G Series, Dell Precision, Latitude
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000220264/dsa-2023-412-dell-technologies-powerprotect-security-update-for-multiple-security-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000216234/dsa-2023-180-security-update-for-intel-product-update-2023-3-advisories

Affected Product	**Palo Alto**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38802, CVE-2023-6790, CVE-2023-6792, CVE-2023-6793, CVE-2023-6794, CVE-2023-6795, CVE-2023-6789, CVE-2023-6791)
Description	Palo Alto has released security updates addressing multiple security vulnerabilities identified in Palo Alto Networks PAN-OS software, impacting various aspects of product functionality. The vulnerabilities range in severity, with potential consequences including denial-of-service (DoS) attacks, cross-site scripting (XSS) exploits, arbitrary file uploads, OS command injections, plaintext disclosure of external system integration credentials, and stored XSS vulnerabilities. It is highly recommended to apply necessary security fixes at earliest to avoid issues
Affected Products	PAN-OS 8.1 to 8.1.24-h1 PAN-OS 8.1 to 8.1.26 PAN-OS 9.0 to 9.0.17 PAN-OS 9.0 to 9.0.17-h4 PAN-OS 9.0 to 9.0.17-h1 PAN-OS 9.1 to 9.1.17 PAN-OS 9.1 to 9.1.16-h3 PAN-OS 10.2 to 10.2.6 PAN-OS 10.2 to 10.2.5 PAN-OS 10.0 All PAN-OS 10.0 to 10.0.12 PAN-OS 10.1 to 10.1.11 PAN-OS 10.1 to 10.1.9 PAN-OS 10.2 to 10.2.4 PAN-OS 11.0 to 11.0.3 Prisma Access Customers whose most recent software upgrade was before 09/30 Prisma SD-WAN ION 6.2 to 6.2.3 Prisma SD-WAN ION 6.1 to 6.1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2023-38802 https://security.paloaltonetworks.com/CVE-2023-6790 https://security.paloaltonetworks.com/CVE-2023-6792 https://security.paloaltonetworks.com/CVE-2023-6793 https://security.paloaltonetworks.com/CVE-2023-6794 https://security.paloaltonetworks.com/CVE-2023-6795 https://security.paloaltonetworks.com/CVE-2023-6789 https://security.paloaltonetworks.com/CVE-2023-6791

Affected Product	**CPanel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46219, CVE-2023-46218)
Description	CPanel has released security updates addressing vulnerabilities in libcurl product. **CVE-2023-46219** - When saving HSTS data to an excessively long file name, curl could end up removing all contents, making subsequent requests using that file unaware of the HSTS status they should otherwise use. **CVE-2023-46218** - This flaw allows a malicious HTTP server to set "super cookies" in curl that are then passed back to more origins than what is otherwise allowed or possible CPanel recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	All versions of libcurl through 8.4.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2023-12-13-maintenance-and-security-release/

Affected Product	**HPE**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-22045, CVE-2023-22041, CVE-2023-22036, CVE-2023-22081, CVE-2023-22049)
Description	HPE has released security updates addressing security vulnerabilities identified in HPE Intelligent Management Center. These vulnerabilities could be remotely exploited to allow code execution, unauthorized data access and denial of service. It is recommended to apply necessary security fixes at earliest to avoid issues
Affected Products	HPE Intelligent Management Center (iMC) - Prior to 7.3 E0710H02
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04574en_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.