Advisory Alert

Alert Number: AAA20230921 **Date:** September 21, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Cpanel	**High**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
HP	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2007-4559, CVE-2016-20012, CVE-2020-14145, CVE-2020-15778, CVE-2021-36368, CVE-2022-0778, CVE-2022-1292, CVE-2022-1587, CVE-2022-2068, CVE-2022-2097, CVE-2022-3566, CVE-2022-40982, CVE-2022-4304, CVE-2022-45884, CVE-2022-45885, CVE-2022-45886, CVE-2022-45887, CVE-2022-45919, CVE-2023-0001, CVE-2023-0286, CVE-2023-0459, CVE-2023-1255, CVE-2023-1380, CVE-2023-20569, CVE-2023-20867, CVE-2023-2176, CVE-2023-21930, CVE-2023-21937, CVE-2023-21938, CVE-2023-21939, CVE-2023-2194, CVE-2023-21954, CVE-2023-21967, CVE-2023-21968, CVE-2023-2269, CVE-2023-2454, CVE-2023-2455, CVE-2023-2513, CVE-2023-2603, CVE-2023-2650, CVE-2023-26555, CVE-2023-2828, CVE-2023-28466, CVE-2023-28709, CVE-2023-28840, CVE-2023-28842, CVE-2023-2953, CVE-2023-2976, CVE-2023-31084, CVE-2023-3138, CVE-2023-31436, CVE-2023-32269, CVE-2023-34462, CVE-2023-3567, CVE-2023-3609, CVE-2023-3611, CVE-2023-3635, CVE-2023-3817, CVE-2023-38408)
Description	Dell has released a security update addressing multiple critical vulnerabilities that exist in third party products that in turn affect Dell products. Successful exploitation of these vulnerabilities could lead to Race condition, Denial of service, Privilege Escalation, Information Exposure. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell Secure Connect Gateway Versions 5.12.00.10, 5.14.00.16, 5.16.00.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000217814/dsa-2023-305-security-update-for-dell-secure-connect-gateway-multiple-third-party-component-vulnerabilities

Affected Product	**Cpanel**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38039, CVE-2023-4807)
Description	Cpanel has released security updates addressing multiple vulnerabilities that exist EasyApache 4. **CVE-2023-38039** - When curl retrieves an HTTP response, it stores the incoming headers so that they can be accessed later via the libcurl headers API. However, curl did not have a limit in how many or how large headers it would accept in a response, allowing a malicious server to stream an endless series of headers and eventually cause curl to run out of heap memory. **CVE-2023-4807** - An Improper input validation vulnerability exists due to insufficient validation of user-supplied input within the POLY1305 MAC (message authentication code) implementation. A remote attacker can send specially crafted input to the application and corrupt MM registers on Windows 64 platform, resulting in a denial of service condition. Cpanel recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	cPanel with EasyApache 4 running on All versions of libcurl through 8.2.1. and OpenSSL through 1.1.1v.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2023-09-20-maintenance-and-security-release/

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40284, CVE-2023-3354, CVE-2023-2002, CVE-2023-3090, CVE-2023-3390, CVE-2023-3776, CVE-2023-4004, CVE-2023-20593, CVE-2023-35001, CVE-2023-35788)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Denial of service, Privilege escalation, Arbitrary read and write, Sensitive information disclosure. Redhat recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 8.8 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:5264 https://access.redhat.com/errata/RHSA-2023:5244 https://access.redhat.com/errata/RHSA-2023:5239

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-36402, CVE-2023-2007, CVE-2023-20588, CVE-2023-34319, CVE-2023-3772, CVE-2023-3812, CVE-2023-3863, CVE-2023-40283, CVE-2023-4128, CVE-2023-4132, CVE-2023-4133, CVE-2023-4134, CVE-2023-4194, CVE-2023-4385, CVE-2023-4387, CVE-2023-4459, CVE-2022-38457, CVE-2022-40133, CVE-2023-3610, CVE-2023-37453, CVE-2023-4147, CVE-2023-4273, CVE-2023-4459, CVE-2023-4563, CVE-2023-4569)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to multiple security flaws. Suse recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Basesystem Module 15-SP5 Development Tools Module 15-SP5 Legacy Module 15-SP5 openSUSE Leap 15.5 SUSE Linux Enterprise Desktop 15 SP5 SUSE Linux Enterprise High Availability Extension 12 SP5, 15 SP5 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5, 15-SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15-SP5 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5 SUSE Linux Enterprise Workstation Extension 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233705-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233704-1/

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20867, CVE-2023-20883, CVE-2023-21930, CVE-2023-21954, CVE-2023-21967, CVE-2023-21939, CVE-2023-21937, CVE-2023-21938, CVE-2023-21968, CVE-2023-2976, CVE-2023-33201, CVE-2023-34981, CVE-2023-39252, CVE-2023-20594, CVE-2023-20597)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products that in turn affect Dell products. Successful exploitation of these vulnerabilities could lead to lead to multiple security flaws. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	BIOS Versions prior to 2.10.2 of • Dell PowerEdge R6515 • Dell PowerEdge R6525 • Dell PowerEdge R7515 • Dell PowerEdge R7525 • Dell PowerEdge C6525 • Dell PowerEdge XE8545 • Dell EMC XC Core XC7525 Dell SCG Policy Manager 5.16.00.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000217781/dsa-2023-348-security-update-for-dell-amd-based-poweredge-server-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000217683/dsa-2023-321-security-update-for-dell-secure-connect-gateway-security-policy-manager-vulnerabilities

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20594, CVE-2023-20597)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to disclosure of sensitive information. HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE ProLiant XL675d Gen10 Plus Server - Prior to v2.64_11-30-2022 HPE ProLiant XL645d Gen10 Plus Server - Prior to v2.64_11-30-2022 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to v2.64_11-30-2022 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to v2.64_11-17-2022 HPE ProLiant DL345 Gen10 Plus server - Prior to v2.64_11-17-2022 HPE ProLiant DL365 Gen10 Plus server - Prior to v2.64_11-17-2022 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to v2.64_11-17-2022
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04541en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04537en_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.