Advisory Alert

Alert Number: **AAA20240904** **Date:** **September 4, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Insufficient Verification Of Data Authenticity
Dell	**High**	Improper Isolation Vulnerability
HPE	**High**	Local Escalation Of Privilege Vulnerability
VMware Broadcom	**High**	Code-Execution Vulnerability
Red Hat	**High ,** **Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Insufficient Verification of Data Authenticity (CVE-2024-39689)
Description	IBM has released security updates addressing an Insufficient Verification of Data Authenticity flaw that exists in IBM Security QRadar EDR. A flaw in Certifi's python-certifi package could provide weaker than expected security, caused by the use of the GLOBALTRUST root certificate. An attacker could exploit this vulnerability to launch further attacks on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar EDR 3.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7167122

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Improper Isolation Vulnerability (CVE-2023-49141)
Description	Dell has released security updates addressing an Improper Isolation Vulnerability that exists in Intel Processor Stream Cache, which in turn affects Dell Precision Rack. **CVE-2023-49141 -** Improper isolation in some Intel Processors stream cache mechanism may allow an authenticated user to potentially enable escalation of privilege via local access. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Precision 7960 Rack Versions prior to 2.2.8 Precision 7960 XL Rack Versions prior to 2.2.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000228048/dsa-2024-370

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Local Escalation of Privilege Vulnerability (CVE-2024-24853)
Description	HPE has released security updates addressing a Local Escalation of Privilege Vulnerability that exists in their products. **CVE-2024-24853** - Incorrect behavior order in transition between executive monitor and SMI transfer monitor (STM) in some Intel(R) Processor may allow a privileged user to potentially enable escalation of privilege via local access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant DL20 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.20_08-07-2024 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant ML30 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to v2.20_08-07-2024 HPE ProLiant MicroServer Gen10 Plus - Prior to v3.40_08-01-2024 HPE ProLiant ML30 Gen10 Server - Prior to v3.40_08-01-2024 HPE ProLiant DL20 Gen10 Server - Prior to v3.40_08-01-2024 HPE ProLiant DL160 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant DL180 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant DL360 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant DL380 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant DL560 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant DL580 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant ML110 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant ML350 Gen10 Server - Prior to v3.30_07-31-2024 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.20_08-07-2024 HPE Synergy 660 Gen10 Compute Module - Prior to v3.30_07-31-2024 HPE Synergy 480 Gen10 Compute Module - Prior to v3.30_07-31-2024 HPE ProLiant BL460c Gen10 Server Blade - Prior to v3.30_07-31-2024 HPE Apollo 4200 Gen10 Plus System - Prior to v2.20_08-07-2024 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.20_08-07-2024 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.20_08-07-2024 HPE Apollo 4200 Gen10 Server - Prior to v3.30_07-31-2024 HPE Apollo 4510 Gen10 System - Prior to v3.30_07-31-2024 HPE ProLiant XL170r Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant XL190r Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant e910 Server Blade - Prior to v3.30_07-31-2024 HPE ProLiant e910t Server Blade - Prior to v3.30_07-31-2024 HPE Edgeline e920 Server Blade - Prior to v2.20_08-07-2024 HPE Edgeline e920d Server Blade - Prior to v2.20_08-07-2024 HPE Edgeline e920t Server Blade - Prior to v2.20_08-07-2024 HPE ProLiant m750 Server Blade - Prior to v3.40_08-01-2024 HPE StoreEasy 1660 Storage - Prior to v2.20_08-07-2024 (U46 ROM Family), v3.30_07-31-2024 (U30 ROM Family) HPE StoreEasy 1860 Storage - Prior to v2.20_08-07-2024 (U46 ROM Family), v3.30_07-31-2024 (U30 ROM Family) HPE Storage File Controller - Prior to v3.30_07-31-2024 HPE Storage Performance File Controller - Prior to v3.30_07-31-2024 HPE StoreEasy 1460 Storage - Prior to v3.30_07-31-2024 HPE StoreEasy 1560 Storage - Prior to v3.30_07-31-2024 HPE StoreEasy 1660 Expanded Storage - Prior to v3.30_07-31-2024 HPE StoreEasy 1660 Performance Storage - Prior to v3.30_07-31-2024 HPE StoreEasy 1860 Performance Storage - Prior to v3.30_07-31-2024 HPE StoreEasy 1650 Expanded Storage - Prior to v2.20_08-07-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04681en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesb3p04694en_us&docLocale=en_US#resolution

Affected Product	**VMware Broadcom**
Severity	**High**
Affected Vulnerability	Code-execution Vulnerability (CVE-2024-38811)
Description	Broadcom has released security updates addressing a Code-Execution Vulnerability that exists in VMware Fusion. **CVE-2024-38811-** VMware Fusion contains a code-execution vulnerability due to the usage of an insecure environment variable. A malicious actor with standard user privileges may exploit this vulnerability to execute code. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Fusion 13.x running on MacOS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24939

Affected Product	**Red Hat**
Severity	**High , Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26946, CVE-2024-35839, CVE-2024-35875, CVE-2024-35895, CVE-2024-38540, CVE-2024-38570, CVE-2024-39502, CVE-2024-40914, CVE-2024-40956, CVE-2024-40978, CVE-2024-40983, CVE-2024-41044, CVE-2024-42102, CVE-2024-42131, CVE-2022-48799, CVE-2024-40995, CVE-2024-41090, CVE-2024-41091)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Use After Free, Denial Of Service, Improper Input Validation. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64 Red Hat Enterprise Linux Server - TUS 8.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:6267 • https://access.redhat.com/errata/RHSA-2024:6268 • https://access.redhat.com/errata/RHSA-2024:6156

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.