Advisory Alert

Alert Number: AAA20240723 **Date:** July 23, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Buffer Overflow Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Red Hat	**High**	Use-after-free Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Zimbra	**High**	Security Update
IBM	**High**, Medium	Multiple Vulnerabilities
Check Point	Low	Blast-RADIUS Attack

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2021-38578)
Description	HPE has released security updates addressing a Buffer Overflow Vulnerability that exists in their products. **CVE-2021-38578** - Existing CommBuffer checks in SmmEntryPoint will not catch underflow when computing BufferSize. The vulnerability could be remotely exploited to allow Out-of-Bounds write vulnerability. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Alletra 4110 - Prior to v2.20_05-27-2024 HPE Alletra 4120 - Prior to v2.20_05-27-2024 HPE ProLiant DL20 Gen11 - Prior to v1.48_03-14-2024 HPE ProLiant DL110 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DL325 Gen11 Server - Prior to v1.60_03-14-2024 HPE ProLiant DL345 Gen11 Server - Prior to v1.60_03-14-2024 HPE ProLiant ML350 Gen11 Server - Prior to v2.20_05-27-2024 HPE ProLiant DL360 Gen11 Server - Prior to v2.20_05-27-2024 HPE ProLiant DL365 Gen11 Server - Prior to v1.60_03-14-2024 HPE ProLiant DL380 Gen11 Server - Prior to v2.20_05-27-2024 HPE ProLiant DL385 Gen11 Server - Prior to v1.60_03-14-2024 HPE ProLiant DL380a Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DL560 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant ML30 Gen11 - Prior to v1.48_03-14-2024 HPE ProLiant MicroServer Gen11 - Prior to v1.48_03-14-2024 HPE ProLiant DL20 Gen10 Plus server - Prior to v2.10_03-21-2024 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.10_05-27-2024 HPE ProLiant DL325 Gen10 Plus server - Prior to v3.10_03-21-2024 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to v3.10_03-21-2024 HPE ProLiant DL345 Gen10 Plus server - Prior to v3.10_03-21-2024 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.10_05-27-2024 HPE ProLiant DL365 Gen10 Plus server - Prior to v3.10_03-21-2024 HPE ProLiant DL385 Gen10 Plus server - Prior to v3.10_03-21-2024 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.10_05-27-2024 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to v3.10_03-21-2024 HPE ProLiant ML30 Gen10 Plus server - Prior to v2.10_03-21-2024 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to v2.10_03-21-2024 HPE ProLiant DL20 Gen10 Server - Prior to v3.10_03-21-2024 HPE ProLiant DL160 Gen10 Server - Prior to v3.20_05-27-2024 HPE ProLiant DL180 Gen10 Server - Prior to v3.20_05-27-2024 HPE ProLiant DL325 Gen10 Server - Prior to v3.10_03-21-2024 HPE ProLiant DL360 Gen10 Server - Prior to v3.20_05-27-2024 HPE ProLiant DL380 Gen10 Server - Prior to v3.20_05-27-2024 HPE ProLiant DL385 Gen10 Server - Prior to v3.10_03-21-2024 HPE ProLiant DL560 Gen10 Server - Prior to v3.20_05-27-2024 HPE ProLiant ML30 Gen10 Server - Prior to v3.10_03-21-2024 HPE ProLiant ML110 Gen10 Server - Prior to v3.20_05-27-2024 HPE ProLiant ML350 Gen10 Server - Prior to v3.20_05-27-2024 HPE Synergy 480 Gen11 Compute Module - Prior to v2.20_05-27-2024 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.10_05-27-2024 HPE ProLiant BL460c Gen10 Server Blade - Prior to v3.20_05-27-2024 HPE Synergy 480 Gen10 Compute Module - Prior to v3.20_05-27-2024 HPE Synergy 660 Gen10 Compute Module - Prior to v3.20_05-27-2024 HPE Apollo 2000 Gen10 Plus System - Prior to v2.10_05-27-2024 HPE Apollo 4200 Gen10 Plus System - Prior to v2.10_05-27-2024 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.10_05-27-2024 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to v3.10_03-21-2024 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.10_05-27-2024 HPE ProLiant XL645d Gen10 Plus Server - Prior to v3.10_03-21-2024 HPE ProLiant XL675d Gen10 Plus Server - Prior to v3.10_03-21-2024 HPE ProLiant XL170r Gen10 Server - Prior to v3.20_05-27-2024 HPE ProLiant XL190r Gen10 Server - Prior to v3.20_05-27-2024 HPE ProLiant e910 Server Blade - Prior to v3.20_05-27-2024 HPE ProLiant e910t Server Blade - Prior to v3.20_05-27-2024 HPE Edgeline e920t Server Blade - Prior to v2.10_05-27-2024 HPE Edgeline e920 Server Blade - Prior to v2.10_05-27-2024 HPE Edgeline e920d Server Blade - Prior to v2.10_05-27-2024 HPE Compute Edge Server e930t - Prior to v2.20_05-27-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04671en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2013-7285, CVE-2019-10173, CVE-2021-21342, CVE-2021-21344, CVE-2021-21345, CVE-2021-21346, CVE-2021-21347, CVE-2021-21350, CVE-2021-21351, CVE-2021-43113)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell Protection Advisor. 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	Dell Protection Advisor Versions 19.8,19.9 and 19.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000227136/dsa-2024-053-security-update-for-data-protection-advisor-multiple-third-party-component-vulnerabilities

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33078, CVE-2021-33077, CVE-2021-33080, CVE-2021-33074, CVE-2021-33069, CVE-2021-33075, CVE-2021-33083, CVE-2021-33082)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell Flash Storage firmware. 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	Systems running on Dell Express Flash NVMe P4800X PCIe SSD firmware Versions before E2010600
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000199271/dsa-2022-128

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Use-after-free Vulnerability (CVE-2024-36886)
Description	Red Hat has released security updates addressing a Use-after-free Vulnerability that exists in Red Hat Enterprise Linux 9. **CVE-2024-36886** - A use-after-free (UAF) flaw exists in the Linux Kernel within the reassembly of fragmented TIPC messages, specifically in the tipc_buf_append() function. The issue results due to a lack of checks in the error handling cleanup and can trigger a UAF on "struct sk_buff", which may lead to remote code execution. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:4713

Affected Product	**SUSE**	
Severity	**High**	
Affected Vulnerability	Multiple vulnerabilities	
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, data corruption, out-of-bounds access, use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.	
Affected Products	Basesystem Module 15-SP6 Development Tools Module 15-SP6 Legacy Module 15-SP6 openSUSE Leap 15.6 SUSE Linux Enterprise Desktop 15 SP6 SUSE Linux Enterprise High Availability Extension 15 SP6	SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Workstation Extension 15 SP6
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20242571-1/	

Affected Product	**Zimbra**
Severity	**High**
Affected Vulnerability	Security Update
Description	Zimbra has released security updates addressing multiple vulnerabilities including Remote Code Execution, High Severity Infinite Loop and Prototype Pollution that are associated with the outdated third party products that are used in Zimbra products. Zimbra advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Zimbra Daffodil versions prior to 10.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0#What's_New

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27088, CVE-2024-27982, CVE-2024-27983, CVE-2024-28863, CVE-2024-29415)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar Pulse App. Exploitation of these vulnerabilities may lead to Denial of Service, Security Bypass, Cross-site Scripting and Server-side Request Forgery. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Pulse App versions 1.0.0 - 2.2.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7160858

Affected Product	**Check Point**
Severity	**Low**
Affected Vulnerability	Blast-RADIUS Attack (CVE-2024-3596)
Description	Check Point has released a workaround addressing the Blast-RADIUS attack that exists in their products. **CVE-2024-3596** - The Blast-RADIUS attack allows a man-in-the-middle attacker between the RADIUS client and server to forge a valid protocol accept message in response to a failed authentication request. This forgery could give the attacker access to network devices and services without the attacker guessing or brute forcing passwords or shared secrets. The attacker does not learn user credentials. Check Point advises to apply the mitigations at your earliest to protect systems from potential threats.
Affected Products	Multi-Domain Security Management, Quantum Security Gateways, Quantum Security Management versions R81, R81.10, R81.20
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk182516

Disclaimer