Advisory Alert

Alert Number: AAA20240531 **Date:** May 31, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE- 2018-15919, CVE- 2019-6109, CVE- 2019-6110, CVE- 2019-6111, CVE- 2018-20685, CVE- 2020-15778, CVE- 2020-14145, CVE- 2020-12062, CVE- 2021-41617, CVE- 2023-38408, CVE- 2023- 48795)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in OpenSSH, that impact Junos OS and Junos OS Evolved. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Privilege Escalation, Command Injection, Access Bypass. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS versions greater than or equal to 19.4R1 Junos OS Evolved versions greater than or equal to 22.3R1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-05-Reference-Advisory-Junos-OS-and-Junos-OS-Evolved-Multiple-CVEs-reported-in-OpenSSH

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in SUSE Linux Kernel. These vulnerabilities could be exploited by malicious users to cause Use After Free, NULL Pointer Dereference, Denial Of Service. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Availability Extension 12 SP5 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20241870-1

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45733, CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237, CVE-2021-38575)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Unauthorized Access, Remote Code Execution, Denial of Service, Buffer Overflow. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Alletra 4110 - Prior to v2.16_03-01-2024 HPE Alletra 4120 - Prior to v2.16_03-01-2024 HPE Apollo 2000 Gen10 Plus System - Prior to v2.00_02-22-2024 HPE Apollo 2000 System - Prior to v3.10_02-22-2024 HPE Apollo 4200 Gen10 Plus System - Prior to v2.00_02-22-2024 HPE Compute Edge Server e930t - Prior to v2.16_03-01-2024 HPE Edgeline e920 Server Blade - Prior to v2.00_02-22-2024 HPE Edgeline e920d Server Blade - Prior to v2.00_02-22-2024 HPE Edgeline e920t Server Blade - Prior to v2.00_02-22-2024 HPE ProLiant BL460c Gen10 Server Blade - Prior to v3.10_02-22-2024 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.00_02-22-2024 HPE ProLiant DL110 Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant DL160 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL180 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL20 Gen10 Plus server - Prior to v2.10_05-16-2024 HPE ProLiant DL20 Gen10 Server - Prior to v3.10_03-21-2024 HPE ProLiant DL20 Gen11 - Prior to v1.48_03-14-2024, v1.50_05-16-2024 HPE ProLiant DL20 Gen9 Server - Prior to v3.40_03-21-2024 HPE ProLiant DL320 Gen11 Server - Prior to v2.16_03-01-2024 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DL360 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL360 Gen11 Server - Prior to v2.16_03-01-2024 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DL380 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL380 Gen11 Server - Prior to v2.16_03-01-2024 HPE ProLiant DL380a Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant DL560 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL560 Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant DX170r Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX190r Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX220n Gen10 Plus server - Prior to v2.00_02-22-2024 HPE ProLiant DX360 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DX360 Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX380 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DX380 Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX4200 Gen10 server - Prior to v2.00_02-22-2024 HPE ProLiant DX560 Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant e910 Server Blade - Prior to v3.10_02-22-2024 HPE ProLiant e910t Server Blade - Prior to v3.10_02-22-2024 HPE ProLiant MicroServer Gen10 Plus - Prior to v3.10_05-16-2024 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to v2.10_05-16-2024 HPE ProLiant MicroServer Gen11 - Prior to v1.48_03-14-2024 HPE ProLiant MicroServer Gen11 - Prior to v1.50_05-16-2024 HPE ProLiant ML110 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant ML110 Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant ML30 Gen10 Plus server - Prior to v2.10_05-16-2024 HPE ProLiant ML30 Gen10 Server - Prior to v3.10_05-16-2024 HPE ProLiant ML30 Gen11 - Prior to v1.48_03-14-2024 HPE ProLiant ML30 Gen11 - Prior to v1.50_05-16-2024 HPE ProLiant ML30 Gen9 Server - Prior to v3.40_03-21-2024 HPE ProLiant ML350 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant ML350 Gen11 Server - Prior to v2.16_03-01-2024 HPE ProLiant RL300 Gen11 - Prior to v1.60_03-07-2024 HPE ProLiant XL170r Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant XL190r Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.00_02-22-2024 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.00_02-22-2024 HPE Synergy 480 Gen10 Compute Module - Prior to v3.10_02-22-2024 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.00_02-22-2024 HPE Synergy 480 Gen11 Compute Module - Prior to v2.16_03-01-2024 HPE Synergy 660 Gen10 Compute Module - Prior to v3.10_02-22-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04593en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04637en_us&docLocale=en_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.