Advisory Alert

Alert Number: **AAA20240724** **Date:** **July 24, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Arbitrary Code Execution Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SonicWall	**High**	Blast-RADIUS Attack
F5	**High**	Resource Exhaustion Vulnerability
HPE	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Juniper	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2023-51385)
Description	IBM has released security updates addressing an Arbitrary Code Execution vulnerability that exists in OpenSSH third-party product that in turn affects IBM products. This vulnerability is caused by improper validation of shell metacharacters. By sending a specially crafted request using expansion tokens, an attacker could exploit this vulnerability. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Network Packet Capture 7.5.0 - 7.5.0 Update Package 7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7160961

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-6546, CVE-2024-21823)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-6546** - A race condition was found in the GSM 0710 tty multiplexor in the Linux kernel. This issue occurs when two threads execute the GSMIOC_SETCONF ioctl on the same tty file descriptor with the gsm line discipline enabled, and can lead to a use-after-free problem on a struct gsm_dlci while restarting the gsm mux. This could allow a local unprivileged user to escalate their privileges on the system. **CVE-2024-21823** - Hardware logic with insecure de-synchronization in Intel(R) DSA and Intel(R) IAA for some Intel(R) 4th or 5th generation Xeon(R) processors may allow an authorized user to potentially enable denial of service via local access. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	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 Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:4731 • https://access.redhat.com/errata/RHSA-2024:4729

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Blast-RADIUS Attack (CVE-2024-3596)
Description	SonicWall has released a workaround addressing the Blast-RADIUS attack that exists in their products. **CVE-2024-3596** - The Blast-RADIUS attack enables 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 allow the attacker to access network devices and services without needing to guess or brute-force passwords or shared secrets. The attacker does not gain access to user credentials. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All SonicWall products using RADIUS authentication are affected.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0014

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Resource Exhaustion Vulnerability (CVE-2023-4408)
Description	F5 has released security updates addressing a Resource Exhaustion vulnerability that exists in the BIND third-party product that in turn affects F5 products. **CVE-2023-4408**- The DNS message parsing code in \`named\` includes a section whose computational complexity is overly high. It does not cause problems for typical DNS traffic, but crafted queries and responses may cause excessive CPU load on the affected \`named\` instance by exploiting this flaw. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) 16.1.0 - 16.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000138990

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2017-16137, CVE-2020-23922, CVE-2021-32815, CVE-2021-34334, CVE-2021-34335, CVE-2021-37615, CVE-2021-37616, CVE-2021-37620, CVE-2021-37621, CVE-2021-37622, CVE-2021-37623, CVE-2022-37050, CVE-2022-37051, CVE-2022-37052, CVE-2023-39742, CVE-2023-48161, CVE-2023-48622, CVE-2023-48795, CVE-2023-51385, CVE-2024-21490, CVE-2024-21512, CVE-2024-22443, CVE-2024-22444, CVE-2024-29131, CVE-2024-29133, CVE-2024-33519, CVE-2024-41133, CVE-2024-41134, CVE-2024-41135, CVE-2024-41136, CVE-2024-41914)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service (DoS), Buffer Overflow, Arbitrary Code Execution, Sensitive Information Disclosure. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Unified OSS Console (UOC) - Prior to v3.1.7 HPE Aruba Networking EdgeConnect SD-WAN Gateways running (unless otherwise noted) • ECOS 9.3.x.x: 9.3.3.0 and below • ECOS 9.2.x.x: 9.2.9.0 and below • ECOS 9.1.x.x: 9.1.11.0 and below • ECOS 9.0.x.x: all builds are affected and are out of maintenance. • ECOS 8.x.x.x: all builds are affected and are out of maintenance. HPE Aruba Networking • EdgeConnect SD-WAN Orchestrator (self-hosted, on-premises) • EdgeConnect SD-WAN Orchestrator (self-hosted, public cloud IaaS) • EdgeConnect SD-WAN Orchestrator-as-a-Service • EdgeConnect SD-WAN Orchestrator-SP Tenant Orchestrators • EdgeConnect SD-WAN Orchestrator Global Enterprise Tenant Orchestrators ▪ EdgeConnect SD-WAN Orchestrator 9.4.x: Orchestrator 9.4.1 (all builds) and below ▪ EdgeConnect SD-WAN Orchestrator 9.3.x: Orchestrator 9.3.2 (all builds) and below ▪ EdgeConnect SD-WAN Orchestrator 9.2.x: Orchestrator 9.2.9 (all builds) and below ▪ EdgeConnect SD-WAN Orchestrator 9.1.x: Orchestrator 9.1.9 (all builds) and below ▪ Any older branches of Orchestrator not specifically mentioned
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04670en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04673en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0553, CVE-2023-3817, CVE-2024-28835, CVE-2024-33601, CVE-2023-3446, CVE-2023-6129, CVE-2023-4813, CVE-2023-32233, CVE-2023-35001, CVE-2023-3609, CVE-2023-39615, CVE-2024-0567, CVE-2024-33599, CVE-2024-28834, CVE-2023-5981, CVE-2023-40217, CVE-2023-5156, CVE-2023-38546, CVE-2024-33600, CVE-2024-33602, CVE-2023-3341, CVE-2023-36632, CVE-2024-31905, CVE-2023-0361, CVE-2024-2961, CVE-2023-4806, CVE-2023-5678, CVE-2023-48795)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Sensitive information disclosure, Denial of Service, Privilege Escalation, Buffer overflow. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Network Packet Capture 7.5.0 - 7.5.0 Update Package 7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7160961

Affected Product	**Juniper**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38545, CVE-2023-38546, CVE-2023-23914, CVE-2023-23915, CVE-2020-8284, CVE-2020-8285, CVE-2020-8286, CVE-2018-1000120, CVE-2018-1000122)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could compromise the affected system. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS • All versions before 21.4R3-S8, 23.4R1-S1, 23.4R2 • All versions before 21.4R3-S5, 22.2R3-S2, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4R3. • All versions before 21.2R1 Junos OS Evolved • All versions before 21.4R3-S4-EVO • From 22.1-EVO before 22.1R3-S4-EVO • From 22.3-EVO before 22.3R3-S1-EVO • From 22.4-EVO before 22.4R2-S1-EVO
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-cURL-vulnerabilities-resolved?language=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.