Advisory Alert

Alert Number: **AAA20240509** **Date:** **May 9, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
F5	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
HPE	**Medium**	Terrapin Attack Vulnerability

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0775, CVE-2024-1086, CVE-2024-26622, CVE-2023-5717)
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 Heap out-of-bounds write and Use-After-Free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 15 SP2 SUSE Linux Enterprise Live Patching 15-SP2, 15-SP3 SUSE Linux Enterprise Server 15 SP2 SUSE Linux Enterprise Server for SAP Applications 15 SP2, SP3 OpenSUSE Leap 15.3 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Server 15 SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241554-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241558-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20241562-1

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1973, CVE-2023-4639, CVE-2024-1459)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their Red Hat JBoss Enterprise Application. **CVE-2023-1973 -** A flaw was found in Undertow package. Using the FormAuthenticationMechanism, a malicious user could trigger a Denial of Service by sending crafted requests, leading the server to an OutofMemory error, exhausting the server's memory. **CVE-2023-4639 -** A flaw was found in Undertow, which incorrectly parses cookies with certain value-delimiting characters in incoming requests. This issue could allow an attacker to construct a cookie value to exfiltrate HttpOnly cookie values or spoof arbitrary additional cookie values, leading to unauthorized data access or modification. The main threat from this flaw impacts data confidentiality and integrity. **CVE-2024-1459 -** A path traversal vulnerability was found in Undertow. This issue may allow a remote attacker to append a specially-crafted sequence to an HTTP request for an application deployed to JBoss EAP, which may permit access to privileged or restricted files and directories. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 8.0 for RHEL 8 x86_64, 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:2763 • https://access.redhat.com/errata/RHSA-2024:2764

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-31156, CVE-2024-21793, CVE-2024-26026, CVE-2024-33608 CVE-2024-25560, CVE-2024-32049, CVE-2024-28883, CVE-2024-33612, CVE-2024-32761 CVE-2024-33604, CVE-2024-28889, CVE-2024-27202, CVE-2024-28132)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Cross-site scripting, SQL Injection. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) – Versions 17.1.0 - 17.1.1 / 16.1.0 - 16.1.4 / 15.1.0 - 15.1.10 BIG-IP Next Central Manager – Versions 20.0.1 - 20.1.0 BIG-IP (AFM) – Versions 17.1.0 / 16.1.0 - 16.1.3 / 15.1.0 - 15.1.10 BIG-IP Next CNF – Versions 1.1.0 - 1.1.1 BIG-IP (APM) – Versions 17.1.0 / 16.1.0 - 16.1.4 / 15.1.0 - 15.1.10 APM Clients – Versions 7.2.3 - 7.2.4 BIG-IP Next CNF – Versions 1.2.0 - 1.2.1 BIG-IP Next SPK – Versions 1.5.0 - 1.6.0 BIG-IP (Advanced WAF/ASM) – Versions 17.1.0 - 17.1.1 BIG-IP Next (WAF) – Versions 20.0.1 - 20.1.0 NGINX App Protect WAF – Versions 4.0.0 - 4.8.0 / 3.10.0 - 3.12.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000139404

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2012-6708, CVE-2015-9251, CVE-2020-7656, CVE-2011-4969 CVE-2017-18214, CVE-2022-24785, CVE-2016-4055, CVE-2022-31129)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of service, Traverse directories on the system and Cross-site scripting. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale – Version 5.1.4.0 - 5.1.9.1 (HDFS Transparency 3.1.1 up to and including 3.1.1-16) IBM Storage Scale – Version 5.0.5.0 - 5.1.8.2 (HDFS Transparency 3.2.2 up to and including 3.2.2-5)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7150528 • https://www.ibm.com/support/pages/node/7150527

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2023-48795)
Description	HPE has released security update addressing an Information Disclosure Vulnerability that exists in OpenSSH that in turn affects AOS-CX Switches. The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted, and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking Aruba Switch Models: • Aruba CX 10000 Switch Series • Aruba CX 9300 Switch Series • Aruba CX 8400 Switch Series • Aruba CX 8360 Switch Series • Aruba CX 8325 Switch Series • Aruba CX 8320 Switch Series • Aruba CX 6400 Switch Series • Aruba CX 6300 Switch Series • Aruba CX 6200 Switch Series • Aruba CX 6100 Switch Series • Aruba CX 6000 Switch Series • Aruba CX 4100i Switch Series Using the following Software Branch Versions: AOS-CX 10.13.xxxx: 10.13.1005 and below AOS-CX 10.12.xxxx: 10.12.1021 and below AOS-CX 10.10.xxxx: 10.10.1100 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04646en_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.