Advisory Alert

Alert Number: AAA20260330 **Date:** March 30, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
F5	**Critical**	Remote Code Execution Vulnerability
SUSE	**High**	Multiple Vulnerabilities
NetApp	**High**	Denial of Service Vulnerability
Red Hat	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2024-3884, CVE-2025-4949, CVE-2025-48913, CVE-2026-0603)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their Products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.3 EUS 7.3 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:6011

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2015-20107, CVE-2019-20477, CVE-2020-1747, CVE-2021-29921, CVE-2021-3177)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their Products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Automation versions 1.11.0 & 1.11.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7267801

Affected Product	**F5**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2025-53521)
Description	F5 has released a security update addressing multiple vulnerabilities that exist in their Products. **CVE-2025-53521** - When a BIG-IP APM access policy is configured on a virtual server, specific malicious traffic can lead to Remote Code Execution (RCE). F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP APM versions • 17.5.0 - 17.5.1 • 17.1.0 - 17.1.2 • 16.1.0 - 16.1.6 • 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000156741

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40258, CVE-2025-40297, CVE-2025-68284, CVE-2025-68285, CVE-2025-68813, CVE-2025-71085, CVE-2021-47110, CVE-2025-21738, CVE-2026-23074, CVE-2026-23089, CVE-2026-23191, CVE-2025-38159, CVE-2025-38488, CVE-2025-40284)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Linux Enterprise Server 11 SP4 SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20261100-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261130-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261125-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261099-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261102-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261096-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261101-1/

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2025-24528)
Description	NetApp has released a security update addressing a vulnerability that exist in their products. **CVE-2025-24528** - Multiple NetApp products incorporate Kerberos. Kerberos versions prior to 1.22 are susceptible to a vulnerability which when successfully exploited could lead to addition or modification of data or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20260130-0015

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38180, CVE-2026-23204, CVE-2026-23209, CVE-2024-3884, CVE-2025-48913, CVE-2026-0603)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.1 EUS 7.1 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:6012 https://access.redhat.com/errata/RHSA-2026:6037

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Automation versions 1.11.0 & 1.11.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7267801

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.