Advisory Alert

Alert Number: AAA20260727 **Date:** July 27, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Improper Validation Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**Medium**	XPath vulnerability

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Improper Validation Vulnerability (CVE-2026-39821)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2026-39821:** The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com". IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Storage Scale Versions • 5.2.0.0 - 5.2.3.8 • 6.0.0.0 - 6.0.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7281111

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40026, CVE-2026-53059, CVE-2026-52976, CVE-2026-52950, CVE-2026-53006, CVE-2026-52993)
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 the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	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 & ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le 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 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.8 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.8 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.8 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.8 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.8 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 & Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 & IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.8 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.8 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.8 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.8 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.8 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.8 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.8 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.8 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.8 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:45115 • https://access.redhat.com/errata/RHSA-2026:45192

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-55602, CVE-2026-53550, CVE-2026-48710, CVE-2026-48817, CVE-2026-48818, CVE-2026-54282, CVE-2026-54283, CVE-2026-13676, CVE-2026-12208, CVE-2026-13149, CVE-2026-59887, CVE-2026-59869, CVE-2026-25680, CVE-2026-25681, CVE-2026-27136, CVE-2026-33814, CVE-2026-42502, CVE-2026-42506)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Platform Navigator in IBM Cloud Pak for Integration (CP4I) Versions • 16.1.0 to 16.1.0.26 • 16.1.1 & 16.1.2 • 16.1.3.0 to 16.1.3.7 Automation Assets in IBM Cloud Pak for Integration (CP4I) • 4.0.0-sc2 to 4.0.23-sc2 • 4.1.0, 4.2.0 & 4.4.0 • 4.3.0 to 4.3.5 IBM Storage Scale Versions • 5.2.0.0 - 5.2.3.8 • 6.0.0.0 - 6.0.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7281111 • https://www.ibm.com/support/pages/node/7281107

Vendor	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	22.04, 24.04, 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8610-1 • https://ubuntu.com/security/notices/USN-8575-3 • https://ubuntu.com/security/notices/USN-8609-1 • https://ubuntu.com/security/notices/USN-8608-1 • https://ubuntu.com/security/notices/USN-8607-1 • https://ubuntu.com/security/notices/USN-8606-1 • https://ubuntu.com/security/notices/USN-8595-2 • https://ubuntu.com/security/notices/USN-8605-1 • https://ubuntu.com/security/notices/USN-8604-1 • https://ubuntu.com/security/notices/USN-8603-1

Vendor	**F5**
Severity	**Medium**
Affected Vulnerability	XPath vulnerability (CVE-2026-32287)
Description	F5 has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-32287:** Boolean XPath expressions that evaluate to true can cause an infinite loop in logicalQuery.Select, leading to 100% CPU usage. This can be triggered by top-level selectors such as "1=1" or "true()". F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• BIG-IP Next CNF - Versions 1.4.0 - 1.4.1 • BIG-IP Next for Kubernetes - Versions 2.1.0 - 2.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000162380

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.