Advisory Alert

Alert Number: AAA20260605 **Date:** June 5, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
F5	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities
PHP	**Medium**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42264, CVE-2026-42044, CVE-2026-42043)
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. **CVE-2026-42264:** Axios is a promise based HTTP client for the browser and Node.js. fFive config properties (auth, baseURL, socketPath, beforeRedirect, and insecureHTTPParser) in the HTTP adapter are read via direct property access without hasOwnProperty guards, making them exploitable as prototype pollution gadgets. When Object.prototype is polluted by another dependency in the same process, axios silently picks up these polluted values on every outbound HTTP request. **CVE-2026-42044:** Axios is a promise based HTTP client for the browser and Node.js. Axios library is vulnerable to a Prototype Pollution "Gadget" attack that allows any Object.prototype pollution in the application's dependency tree to be escalated into surgical, invisible modification of all JSON API responses — including privilege escalation, balance manipulation, and authorization bypass. **CVE-2026-42043:** Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, an attacker who can influence the target URL of an Axios request can use any address in the 127.0.0.0/8 range (other than 127.0.0.1) to completely bypass the NO_PROXY protection. This vulnerability is due to an incomplete for CVE-2025-62718. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Security SOAR Versions: • 51.0.9.2 • 51.0.9.1 • 51.0.9.0 • 51.0.8.2 • 51.0.8.1 • 51.0.8.0 • 51.0.7.2 • 51.0.7.1 • 51.0.7.0 • 51.0.6.2 • 51.0.6.1 • 51.0.6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7275143 • https://www.ibm.com/support/pages/node/7275142

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46300, CVE-2026-46333, CVE-2026-46243, CVE-2025-38653, CVE-2025-68366, CVE-2026-31613, CVE-2026-31709, CVE-2026-43329, CVE-2026-43322)
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 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux 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 Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.2 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.2 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.2 aarch64 Red Hat CodeReady Linux Builder for x86_64 10 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.2 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.2 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.2 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 10.2 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 10.2 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 10.2 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x 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 ARM 64 - Extended Life Cycle 8.10 aarch64 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-2026:23471 • https://access.redhat.com/errata/RHSA-2026:23470 • https://access.redhat.com/errata/RHSA-2026:23469 • https://access.redhat.com/errata/RHSA-2026:23468 • https://access.redhat.com/errata/RHSA-2026:23395 • https://access.redhat.com/errata/RHSA-2026:23329 • https://access.redhat.com/errata/RHSA-2026:23258

Vendor	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39817, CVE-2025-38085)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-39817**: In the Linux Kernel: fix huge_pmd_unshare() vs GUP-fast race huge_pmd_unshare() drops a reference on a page table that may have previously been shared across processes, potentially turning it into a normal page table used in another process in which unrelated VMAs can afterwards be installed. If this happens in the middle of a concurrent gup_fast(), gup_fast() could end up walking the page tables of another process. While I don't see any way in which that immediately leads to kernel memory corruption, it is really weird and unexpected. **CVE-2025-38085**: In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix huge_pmd_unshare() vs GUP-fast race huge_pmd_unshare() drops a reference on a page table that may have previously been shared across processes, potentially turning it into a normal page table used in another process in which unrelated VMAs can afterwards be installed. If this happens in the middle of a concurrent gup_fast(), gup_fast() could end up walking the page tables of another process. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	F5OS-A Versions: • 1.8.0 - 1.8.4 • 1.5.1 - 1.5.4 F5OS-C Versions: • 1.8.0 - 1.8.2 • 1.6.0 - 1.6.4 Traffix SDC Version: 5.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000161577 • https://my.f5.com/manage/s/article/K000161578

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42033, CVE-2026-42034, CVE-2026-42035, CVE-2026-42036, CVE-2026-42037, CVE-2026-42038, CVE-2026-42039, CVE-2026-42040, CVE-2026-42041, CVE-2026-42042)
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	IBM Security SOAR Versions: • 51.0.9.2 • 51.0.9.1 • 51.0.9.0 • 51.0.8.2 • 51.0.8.1 • 51.0.8.0 • 51.0.7.2 • 51.0.7.1 • 51.0.7.0 • 51.0.6.2 • 51.0.6.1 • 51.0.6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7275143 • https://www.ibm.com/support/pages/node/7275142

Vendor	**PHP**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-44927, CVE-2026-44928)
Description	PHP has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-44927:** In uriparser before 1.0.2, there is pointer difference truncation to int in various places **CVE-2026-44928:** In uriparser before 1.0.2, the function family EqualsUri can misclassify two unequal URIs as equal PHP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PHP Versions prior to 8.5.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/ChangeLog-8.php#8.5.7

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.