Advisory Alert

Alert Number: AAA20260109 **Date:** January 9, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
F5	**High**	Local Denial of Service Vulnerability

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-12543, CVE-2024-3884, CVE-2025-9784)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exists in their products. **CVE-2025-12543**: Undertow fails to validate malformed Host headers, allowing attackers to manipulate server routing or caching logic. This enables Cache Poisoning to serve malicious content to users or SSRF to access restricted internal services. **CVE-2024-3884**: A memory allocation flaw in the form-parsing logic allows attackers to send oversized data via application/x-www-form-urlencoded. This triggers an OutOfMemory (OOM) error in the JVM, crashing the application and rendering it unresponsive. The result is a total Denial of Service by exhausting available system memory. **CVE-2025-9784**: The "MadeYouReset" flaw exploits HTTP/2 stream resets to bypass concurrency limits by forcing the server to issue resets while backend threads continue processing. Attackers can flood the server with "ghost" requests, exhausting CPU and memory to cause a massive Denial of Service. This allows a single connection to bypass standard MAX_CONCURRENT_STREAMS protections. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Application Platform 8.1 for RHEL 9 x86_64 JBoss Enterprise Application Platform 8.1 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:0386 • https://access.redhat.com/errata/RHSA-2026:0384 • https://access.redhat.com/errata/RHSA-2026:0383

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Local Denial of Service Vulnerability (CVE-2023-53178)
Description	F5 has released a security update addressing a local denial of service vulnerability that exists in F5OS and Traffix SDC. **CVE-2023-53178**: A local unprivileged user may exploit this vulnerability and cause data integrity issues or system instability under specific conditions. 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 to 1.8.3 and 1.5.1 to 1.5.4 F5OS-C versions 1.8.0 to 1.8.2 and 1.6.0 to 1.6.4 Traffix SDC versions 5.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000159018

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.