Advisory Alert

Alert Number: AAA20260706 **Date:** July 6, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
F5	**Medium**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23455, CVE-2026-43125, CVE-2026-46090, CVE-2026-45852)
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 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 Server - Extended Life Cycle Support 7 x86_64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x • Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:35844

Vendor	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-58181, CVE-2025-47914)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-58181:** SSH servers parsing GSSAPI authentication requests do not validate the number of mechanisms specified in the request, allowing an attacker to cause unbounded memory consumption. **CVE-2025-47914:** SSH Agent servers do not validate the size of messages when processing new identity requests, which may cause the program to panic if the message is malformed due to an out of bounds read. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next for Kubernetes versions 2.0.0 - 2.1.0 BIG-IP Next SPK versions: • 2.0.0 - 2.0.2 • 1.7.0 - 1.7.15 • 1.9.0 - 1.9.2 BIG-IP Next CNF versions: • 2.0.0 - 2.0.2 • 2.1.0 • 1.1.0 - 1.4.0 FSOC-A versions: • 1.8.0 - 1.8.3 • 1.5.1 - 1.5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000162049 https://my.f5.com/manage/s/article/K000162045

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.