Advisory Alert

Alert Number: AAA20240604 **Date:** June 4, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-23445, CVE-2024-1233, CVE-2024-28752)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in JBoss Enterprise Application Platform. **CVE-2021-23445** - An improper neutralization of input vulnerability was found in datatables.net. If an array is passed to the HTML escape entities function, it does not have its contents escaped, possibly leading to cross site scripting (XSS). **CVE-2024-1233** - A flaw was found in JwtValidator.resolvePublicKey in JBoss EAP, where the validator checks jku and sends a HTTP request. During this process, no whitelisting or other filtering behavior is performed on the destination URL address, which may result in a server-side request forgery (SSRF) vulnerability. **CVE-2024-28752** - A server-side request forgery (SSRF) vulnerability was found in Apache CXF. This issue occurs in attacks on webservices that take at least one parameter of any type, and when Aegisdatabind is used. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:3563 • https://access.redhat.com/errata/RHSA-2024:3561 • https://access.redhat.com/errata/RHSA-2024:3560 • https://access.redhat.com/errata/RHSA-2024:3559

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47076, CVE-2021-47080)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in Traffix SDC component. **CVE-2021-47076** - RDMA/rxe: Return CQE error if invalid lkey was supplied RXE is missing update of WQE status in LOCAL_WRITE failures. This caused a kernel panic if someone sent an atomic operation with an explicitly wrong lkey. **CVE-2021-47080** - RDMA/core: Prevent divide-by-zero error triggered by the user The user_entry_size is supplied by the user and later used as a denominator to calculate number of entries. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Traffix SDC 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000139877

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.