TLP: WHITE

Advisory Alert

Alert Number: **AAA20231101** **Date:** **November 1, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**High**	Open redirect vulnerability
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	Open redirect vulnerability (CVE-2023-20886)
Description	VMware has released security update addressing open redirect vulnerability in VMware Workspace ONE UEM console.by exploiting this vulnerability A malicious actor may be able to redirect a victim to an attacker and retrieve their SAML response to login as the victim user. VMware recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Workspace ONE UEM Version 2302, 2212, 2209, 2206, 2203
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0025.html

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42795, CVE-2023-45648)
Description	Red Hat has released security update addressing request smuggling and information disclosure vulnerability in Apache Tomcat which affecting Red Hat JBoss Web Server. **CVE-2023-42795-** An information disclosure vulnerability in Apache Tomcat. Tomcat may skip, after an error, the recycling of the internal objects that the next request/response process might use, resulting in information leaking from one request to the next. **CVE-2023-45648-** A request smuggling vulnerability in Apache Tomcat, where an improper input validation can occur. This flaw allows a malicious user to send a crafted request containing an invalid trailer header, which could be treated as multiple requests, potentially leading to request smuggling when behind a reverse proxy. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	JBoss Enterprise Web Server Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:6207

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.