# Advisory Alert

**Alert Number:** **AAA20240221** **Date:** **February 21, 2024**

|  |  |  |
|---|---|---|
| **Document Classification Level** | : | Public Circulation Permitted \| Public |
| **Information Classification Level** | : | TLP: WHITE |

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **VMware** | **Critical** | Multiple Vulnerabilities |
| **Red Hat** | **High, Medium** | Multiple Vulnerabilities |
| **Joomla** | **High, Medium, Low** | Multiple Vulnerabilities |
| **Ubuntu** | **High, Medium, Low** | Multiple Vulnerabilities |
| **F5** | **Medium** | Information Exposure Through Timing Discrepancy Vulnerability |

## Description

|  |  |
|---|---|
| Affected Product | **VMware** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-22245, CVE-2024-22250) |
| Description | VMware has released a security updates addressing multiple vulnerabilities affecting their products.<br>**CVE-2024-22245** - The VMware Enhanced Authentication Plug-in (EAP) contains an Arbitrary Authentication Relay vulnerability. A malicious actor could trick a target domain user with EAP installed in their web browser into requesting and relaying service tickets for arbitrary Active Directory Service Principal Names (SPNs).<br>**CVE-2024-22250** - The VMware Enhanced Authentication Plug-in (EAP) contains a Session Hijack vulnerability. A malicious actor with unprivileged local access to a windows operating system can hijack a privileged EAP session when initiated by a privileged domain user on the same system.<br>VMware strongly recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | VMware Enhanced Authentication Plug-in (EAP) |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.vmware.com/security/advisories/VMSA-2024-0003.html |

|  |  |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **High, Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2021-33655, CVE-2022-2196, CVE-2022-3239, CVE-2022-3625, CVE-2022-20368, CVE-2022-23960, CVE-2022-29581, CVE-2022-36402, CVE-2022-38096, CVE-2022-38457, CVE-2022-40133, CVE-2023-1074, CVE-2023-6546, CVE-2023-6931, CVE-2023-30456, CVE-2023-31084, CVE-2023-51042, CVE-2024-1086, CVE-2023-44981, CVE-2022-3545, CVE-2022-41858, CVE-2023-1073, CVE-2023-1838, CVE-2023-2166, CVE-2023-2176, CVE-2023-4623, CVE-2023-4921, CVE-2023-5717, CVE-2023-6356, CVE-2023-6535, CVE-2023-6536, CVE-2023-6606, CVE-2023-6610, CVE-2023-6817, CVE-2023-40283, CVE-2023-45871, CVE-2023-46813, CVE-2024-0646) |
| Description | Red Hat has released security updates addressing multiple vulnerabilities. Exploitation of these vulnerabilities by an attacker could lead to Out of boundary write, Use-after-free Condition, Integer overflow, NULL pointer dereference.<br>Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64<br>Red Hat Enterprise Linux Server - AUS 8.6 x86_64<br>Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x<br>Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le<br>Red Hat Virtualization Host 4 for RHEL 8 x86_64<br>Red Hat Enterprise Linux Server - TUS 8.6 x86_64<br>Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64<br>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le<br>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64<br>Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64<br>Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le<br>Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64<br>Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64<br>Red Hat Enterprise Linux for x86_64 8 x86_64<br>Red Hat Enterprise Linux for IBM z Systems 8 s390x<br>Red Hat Enterprise Linux for Power, little endian 8 ppc64le<br>Red Hat Enterprise Linux for ARM 64 8 aarch64<br>Red Hat CodeReady Linux Builder for x86_64 8 x86_64<br>Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le<br>Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://access.redhat.com/errata/RHSA-2024:0930<br>https://access.redhat.com/errata/RHSA-2024:0903<br>https://access.redhat.com/errata/RHSA-2024:0897<br>https://access.redhat.com/errata/RHSA-2024:0876 |

| | |
|---|---|
| Affected Product | **Joomla** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-21726, CVE-2023-21725, CVE-2023-21724, CVE-2023-21723, CVE-2023-21722 ) |
| Description | Joomla has released security updates addressing multiple vulnerabilities. Exploitation of these vulnerabilities could lead to Cross- Site scripting, Open redirect and Insufficient Session Expiration.<br>Joomla recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | Joomla! CMS versions 1.5.0 - 3.10.14-elts, 4.0.0-4.4.2, 5.0.0-5.0.2 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://developer.joomla.org/security-centre/929-20240205-core-inadequate-content-filtering-within-the-filter-code.html<br>https://developer.joomla.org/security-centre/928-20240204-core-xss-in-mail-address-outputs.html<br>https://developer.joomla.org/security-centre/927-20240203-core-xss-in-media-selection-fields.html<br>https://developer.joomla.org/security-centre/926-20240202-core-open-redirect-in-installation-application.html<br>https://developer.joomla.org/security-centre/925-20240201-core-insufficient-session-expiration-in-mfa-management-views.html |

| | |
|---|---|
| Affected Product | **Ubuntu** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-51782, CVE-2023-51780, CVE-2023-7192) |
| Description | Ubuntu has released security updates addressing multiple vulnerabilities. An attacker exploit these vulnerabilities to cause Denial of service (system crash/ memory Exhaustion) or possibly execute Arbitrary code.<br>Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | Ubuntu 16.04<br>Ubuntu 14.04 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://ubuntu.com/security/notices/USN-6646-1<br>https://ubuntu.com/security/notices/USN-6645-1 |

| | |
|---|---|
| Affected Product | **F5** |
| Severity | **Medium** |
| Affected Vulnerability | Information Exposure Through Timing Discrepancy Vulnerability (CVE-2023-47038) |
| Description | F5 has released security updates addressing an Information Exposure Through Timing Discrepancy vulnerability caused due to the difference in response time between malformed ciphertexts in RSA-PSK ClientKeyExchange and ciphertexts with correct PKCS#1 v1.5 padding. By exploiting this vulnerability a remote attacker could perform timing sidechannel attack in RSA-PSK key exchange.<br>F5 recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | BIG-IP Next (all modules) 20.0.1 - 20.0.2<br>BIG-IP Next Central Manager 20.0.1 - 20.0.2 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://my.f5.com/manage/s/article/K000138649 |

**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.**