Advisory Alert

Alert Number: AAA20221026 **Date:** October 26, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
RedHat	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**	Multiple Vulnerabilities
Nginx	**High**	Multiple Vulnerabilities
Samba	**Medium**	Multiple Vulnerabilities
Joomla	**Low**	Multiple Vulnerabilities

Description

Affected Product	**RedHat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-2478, CVE-2021-2479, CVE-2021-2481, CVE-2021-35546, CVE-2021-35575, CVE-2021-35577, CVE-2021-35591, CVE-2021-35596, CVE-2021-35597, CVE-2021-35602, CVE-2021-35604, CVE-2021-35607, CVE-2021-35608, CVE-2021-35610,CVE-2021-35612, CVE-2021-35622, CVE-2021-35623, CVE-2021-35624,CVE-2021-35625, CVE-2021-35626, CVE-2021-35627, CVE-2021-35628,CVE-2021-35630, CVE-2021-35631, CVE-2021-35632, CVE-2021-35633,CVE-2021-35634, CVE-2021-35635, CVE-2021-35636, CVE-2021-35637,CVE-2021-35638, CVE-2021-35639, CVE-2021-35640, CVE-2021-35641, CVE-2021-35642, CVE-2021-35643, CVE-2021-35644, CVE-2021-35645,CVE-2021-35646, CVE-2021-35647,CVE-2021-35648, CVE-2022-21245, CVE-2022-21249, CVE-2022-21253, CVE-2022-21254, CVE-2022-21256, CVE-2022-21264, CVE-2022-21265,CVE-2022-21270, CVE-2022-21278, CVE-2022-21297, CVE-2022-21301, CVE-2022-21302, CVE-2022-21303, CVE-2022-21304, CVE-2022-21339,CVE-2022-21342, CVE-2022-21344, CVE-2022-21348, CVE-2022-21351,CVE-2022-21352, CVE-2022-21358, CVE-2022-21362, CVE-2022-21367,CVE-2022-21368, CVE-2022-21370, CVE-2022-21372, CVE-2022-21374, CVE-2022-21378, CVE-2022-21379,CVE-2022-21412, CVE-2022-21413,CVE-2022-21414, CVE-2022-21415, CVE-2022-21417, CVE-2022-21418, CVE-2022-21423, CVE-2022-21425,CVE-2022-21427, CVE-2022-21435,CVE-2022-21436, CVE-2022-21437, CVE-2022-21438, CVE-2022-21440, CVE-2022-21444, CVE-2022-21451,CVE-2022-21452, CVE-2022-21454,CVE-2022-21457, CVE-2022-21459,CVE-2022-21460, CVE-2022-21462,CVE-2022-21478, CVE-2022-21479,CVE-2022-21509, CVE-2022-21515, CVE-2022-21517,CVE-2022-21522, CVE-2022-21525, CVE-2022-21526, CVE-2022-21527,CVE-2022-21528, CVE-2022-21529,CVE-2022-21530, CVE-2022-21531,CVE-2022-21534, CVE-2022-21537, CVE-2022-21538, CVE-2022-21539,CVE-2022-21547, CVE-2022-21553,CVE-2022-21569, CVE-2022-2850,CVE-2022-0494, CVE-2022-1353, CVE-2022-2588, CVE-2022-23816, CVE-2022-23825, CVE-2022-29900,CVE-2022-29901, CVE-2021-2163, CVE-2021-3715)
Description	RedHat has released patch updates to addressing multiple vulnerabilities that includes in their products. These patch updates includes mysql:8.0 security bug fix, and enhancement update, 389-ds:1.4 security update, kernel-rt security and bug fix update, java-1.8.0-ibm security update and kpatch-patch security updates. Exploitation of the most severe vulnerabilities could cause privilege escalation, Arbitrary code execution and creates a user after free conditions. RedHat highly recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux Server - AUS 7.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 7.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 7.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:7119 https://access.redhat.com/errata/RHSA-2022:7133 https://access.redhat.com/errata/RHSA-2022:7134 https://access.redhat.com/errata/RHSA-2022:6735 https://access.redhat.com/errata/RHSA-2022:7173

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-3153, CVE-2020-3433)
Description	Cisco has released a security update addressing the Multiple Vulnerabilities in the Cisco AnyConnect Secure Mobility Client. These vulnerabilities could allow the attacker to path traversal and execute arbitrary code. In order to carry out this attack, An attacker would need at least valid credentials on the Windows system. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco AnyConnect Secure Mobility Client for Windows releases earlier than 4.8.02042 Cisco AnyConnect Secure Mobility Client for Windows releases earlier than Release 4.9.00086
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-win-path-traverse-qO4HWBsj https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-38185, CVE-2022-1154, CVE-2021-3634)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in the IBM QRadar SIEM product. These vulnerabilities could cause arbitrary code execution, buffer overflow and denial of service. IBM highly recommends to apply necessary fixes at earliest to avoid issues
Affected Products	IBM QRadar SIEM 7.4.0 – 7.4.3 Fix Pack 6 IBM QRadar SIEM 7.5.0 – 7.5.0 Update Pack 2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6831853

Affected Product	**Nginx**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-41741, CVE-2022-41742)
Description	Nginx has issued a patch update to address two vulnerabilities that identified in ngx_http_mp4_module. If exploited, these vulnerabilities could cause worker process crash or worker process memory disclosure. An attacker can exploit these vulnerabilities by sending a specially crafted mp4 file. However the mentioned issues only affect nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the "mp4" directive is used in the configuration file. Nginx highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Nginx 1.1.3+, 1.0.7+.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://mailman.nginx.org/archives/list/nginx-announce@nginx.org/message/RBRRON6PYBJJM2XIAPQBFBVLR4Q6IHRA/

Affected Product	**Samba**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3437, CVE-2022-3592)
Description	Samba has released security updates to address multiple vulnerabilities that exist in multiple versions of Samba. Using these vulnerabilities, A malicious client can use a symlink to escape the exported directory and limit the write heap buffer overflow in the GSSAPI unwrap_des() and unwrap_des3() routines of Heimdal. Samba highly recommended to apply necessary fixes at earliest to avoid issues
Affected Products	All versions of Samba since Samba 4.0 compiled with Heimdal Kerberos All versions of Samba since 4.17.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.samba.org/samba/security/CVE-2022-3437.html https://www.samba.org/samba/security/CVE-2022-3592.html

Affected Product	**Joomla**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-27912, CVE-2022-27913)
Description	Joomla has released patch updates addressing multiple vulnerabilities that exists in their Joomla CMS product. **CVE-2022-27912** – A vulnerability that exists in the Joomla 4 sites with publicly enabled debug mode exposed data of previous requests. **CVE-2022-27913** - Inadequate filtering of potentially malicious user input leads to reflected XSS vulnerabilities in various components. Joomla highly recommends to apply the patch updates at your earliest to avoid issues.
Affected Products	Joomla CMS versions 4.0.0-4.2.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/

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.