NETWORK INTELLIGENCE

The Digital Security Company

January 2023, Edition 1.0

# SECURITY ADVISORY DIGEST

## IN THIS EDITION:

Security Advisory Listing

- Multiple vulnerabilities in VMware vRealize Log Insight
- Multiple vulnerabilities in Google Chrome browser
- Authentication bypass and RCE bugs in Cisco EOL Small Business Routers
- Critical security flaw affects multiple ManageEngine products

Also Inside

**Security Patch Advisory**

Critical High Low

Date: January 27, 2023

# Multiple vulnerabilities in VMware vRealize Log Insight

## BUSINESS IMPACT

Successful exploitation of the vulnerabilities enables attackers to bypass security restrictions, execute arbitrary code, read arbitrary files, perform a denial of service attack and gain unauthorized access to potentially sensitive information.

## RECOMMENDATIONS

1. Update vRealize Log Insight to the latest version. (For instructions – Click here.)

2. Customers who cannot immediately deploy latest updates to vRealize Log Insight can apply the Workaround to temporarily mitigate the vulnerability. (For instructions – Click here.)

## INTRODUCTION

VMware has released fixes to address multiple security bugs (tracked as CVE2022-31706, CVE-2022-31704, CVE-2022-31710 and CVE-2022-31711) in vRealize Log Insight.

Directory traversal vulnerability (CVE-2022-31706) exists in vRealize Log Insight due to an input validation error when processing directory traversal sequences within the vRNI REST API. A remote attacker can send a specially crafted HTTP request and read arbitrary files on the system.
CVSS Score: 9.8

A broken access control vulnerability (CVE-2022-31704) exists in vRealize Log Insight due to improper access restrictions. A remote attacker can bypass implemented security restrictions and execute arbitrary code on the system.
CVSS Score: 9.8

Deserialization vulnerability (CVE-2022-31710) exists in vRealize Log Insight due to insecure input validation when processing serialized data. A remote nonauthenticated attacker can send specially crafted data to the application and perform a denial of service (DoS) attack.
CVSS Score: 7.5 I

Information disclosure vulnerability (CVE-2022-31711) exists in vRealize Log Insight due to excessive data output by the application. A remote attacker can gain unauthorized access to sensitive session and application information.
CVSS Score: 5.3

## AFFECTED PRODUCTS

- VMware vRealize Log Insight: 8.x
- VMware Cloud Foundation (VMware vRealize Log Insight): 4.x and 3.x

## REFERENCES

- VMware fixes critical security bugs in vRealize log analysis tool
- VMware vRealize Log Insight latest updates address multiple security vulnerabilities (CVE-2022-31706, CVE-2022-31704, CVE-2022-31710, CVE-2022-31711)

SECURITY ADVISORY

Date: January 17, 2023

# Multiple vulnerabilities in Google Chrome browser

## BUSINESS IMPACT

Successful exploitation of the vulnerabilities could allow a remote attacker to bypass security restriction, execute arbitrary code or cause denial of service condition on the targeted system, extract sensitive files and plant further malware for disruptive attacks.

## RECOMMENDATIONS

1. Kindly update Google Chrome browser for Windows, Mac and Linux to the latest release.

To verify if the Chrome browser is running latest release, go to Chrome menu > Help > About Google Chrome.

2. Ensure to update Chromium-based browsers such as Microsoft Edge, Opera, and Vivaldi to their latest releases as and when they become available.

## INTRODUCTION

Google has released updates to its Chrome browser for Windows, Mac and Linux to address 17 security fixes.

The vulnerabilities are tracked as CVE-2023-0128, CVE-2023-0129, CVE-2023- 0130, CVE-2023-0131, CVE-2023-0132, CVE-2023-0133, CVE-2023-0134, CVE2023-0135, CVE-2023-0136, CVE-2023-0137, CVE-2023-0138, CVE-2023-0139, CVE-2023-0140 and CVE-2023-0141.

These vulnerabilities exist in Google Chrome for Desktop due to:

- Use after free in Overview Mode and Cart
- Heap buffer overflow in Network Service, Platform Apps and libphonenumber
- Inappropriate implementation in Fullscreen API, iframe Sandbox, Permission prompts and File System API
- Insufficient validation of untrusted input in Downloads • Insufficient policy enforcement in CORS

Imperva researchers recently warned about SymStealer bug (tracked asCVE2022-3656), in Google Chrome and Chromium-based browsers that was patched last October. Researchers say the vulnerability is affecting over 2.5 billion users and can be used to extract sensitive files from affected browsers, such as crypto wallets and cloud provider credentials.

An attacker could exploit these vulnerabilities by creating a specially crafted web page and trick the victim into visiting it.

## AFFECTED PRODUCTS

- Google Chrome versions prior to 109.0.5414.74 (Linux), 109.0.5414.74/.75 (Windows) and 109.0.5414.87 (Mac).

## REFERENCES

- Stable Channel Update for Desktop
- Google Chrome “SymStealer” Vulnerability: How to Protect Your Files from Being Stolen

SECURITY ADVISORY

Date: January 12, 2023

# Authentication bypass and RCE bugs in Cisco EOL Small Business Routers

## BUSINESS IMPACT

Successful exploitation of the vulnerabilities allows a remote attacker to bypass the authentication process, gain root-level privileges, execute arbitrary shell commands, access unauthorized data and plant further malware for disruptive attacks.

## MITIGATIONS

Administrators can mitigate the vulnerabilities by:

- Disabling remote management
- Blocking access to ports 443 and 60443

The routers will still be accessible through the LAN interface after the mitigation has been implemented.

## INTRODUCTION

Cisco is warning its customers of multiple vulnerabilities (tracked as CVE-2023- 20025 and CVE-2023-20026) in Cisco's End-of-Life Small Business Routers that could allow a remote attacker to bypass authentication or execute arbitrary commands on the underlying operating system of an affected device.

The vulnerabilities exist due to improper validation of user input within incoming HTTP packets to the web-based management interface of Cisco Small Business RV016, RV042, RV042G, and RV082 Routers.

A remote non-authenticated attacker can send a specially crafted HTTP request, bypass the authentication process and execute arbitrary commands as root on the affected device.

Proof of Concept exploit code is publicly available for CVE-2023-20025 and CVE2023-20026.

Cisco has not released and will not release software updates to address CVE2023-20025 and CVE-2023-20026 vulnerabilities. Also, there are no workarounds that address these vulnerabilities.

## AFFECTED PRODUCTS

- RV016 Multi-WAN VPN Routers
- RV042 Dual WAN VPN Routers
- RV042G Dual Gigabit WAN VPN Routers
- RV082 Dual WAN VPN Routers

Please note the mentioned router devices are End-of-Life products.

## REFERENCES

- Cisco warns of auth bypass bug with public exploit in EoL routers
- Cisco Small Business RV016, RV042, RV042G, and RV082 Routers Vulnerabilities

SECURITY ADVISORY

Date: January 5, 2023

# Critical security flaw affects multiple ManageEngine products

## BUSINESS IMPACT

Successful exploitation of the vulnerability allows an adversary to execute custom SQL queries with SYSTEM privileges, access the database table entries using the vulnerable request and gain complete control over the affected application.

## INTRODUCTION

Zoho has released fixes to address an SQL Injection vulnerability (CVE-2022- 47523) discovered in ManageEngine's Password Manager Pro, PAM360 and Access Manager Plus.

The vulnerability exists due to insufficient sanitization of user-supplied data. A remote user can send a specially crafted request to the affected application and execute arbitrary SQL commands within the application database. Successful exploitation provides attackers with unauthenticated access to the backend database and allows them to execute custom queries to access database table entries.

State-sponsored attackers are more likely to exploit this ManageEngine bug to backdoor the networks of critical infrastructure organizations.

## RECOMMENDATIONS

1. Ensure Password Manager Pro, PAM360 and Access Manager Plus are updated with latest security patches.

## AFFECTED PRODUCTS

- Password Manager Pro versions 12200 and below
- PAM360 versions 5800 and below
- Access Manager Plus versions 4308 and below

## REFERENCES

- Zoho urges admins to patch critical ManageEngine bug immediately
- SQL Injection Vulnerability - CVE-2022-47523

SECURITY ADVISORY

# Security Patch Advisory

| Severity Matrix | | | |
|---|---|---|---|
| L | M | H | C |
| Low | Medium | High | Critical |

02nd Jan 2023 – 08th Jan 2023
TRAC-ID: NII23.01.0.2

## UBUNTU

| TECHNOLOGIES | ADVISORIES | AFFECTED PRODUCTS | RECOMMENDATION |
|---|---|---|---|
| Ubuntu Linux | USN-5784-1: usbredir vulnerability | • Ubuntu 20.04 LTS<br>• Ubuntu 18.04 LTS<br>• Ubuntu 16.04 ESM<br>• Ubuntu 14.04 ESM | Kindly update to fixed version |
| Ubuntu Linux | USN-5785-1: FreeRADIUS vulnerabilities | • Ubuntu 22.04 LTS<br>• Ubuntu 20.04 LTS<br>• Ubuntu 18.04 LTS<br>• Ubuntu 16.04 ESM | Kindly update to fixed version |

## SUSE

| TECHNOLOGIES | ADVISORIES | AFFECTED PRODUCTS | RECOMMENDATION |
|---|---|---|---|
| SUSE Linux | SUSE-SU2023:0012-1 | • SUSE CaaS Platform 4.0<br>• SUSE Enterprise Storage 6<br>• SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS<br>• SUSE Linux Enterprise Server 15-SP1- LTSS<br>• SUSE Linux Enterprise Server for SAP 15-SP1 | Kindly update to fixed version |
| SUSE Linux | SUSE-SU2023:0011-1 | • SUSE Linux Enterprise Server for SAP 12-SP4<br>• SUSE Linux Enterprise Server for SAP 12-SP5 | Kindly update to fixed version |

SECURITY ADVISORY

# Security Patch Advisory

| Severity Matrix | | | |
|---|---|---|---|
| L | M | H | C |
| Low | Medium | High | Critical |

02nd Jan 2023 – 08th Jan 2023
TRAC-ID: NII23.01.0.2

## ORACLE

| TECHNOLOGIES | ADVISORIES | AFFECTED PRODUCTS | RECOMMENDATION |
|---|---|---|---|
| Oracle Linux | ELSA-2023-0005 | • Oracle Linux 9 (aarch64)<br>• Oracle Linux 9 (x86_64) | **Kindly update to fixed version** |
| Oracle Linux | ELSA-2022- 10108 | • Oracle Linux 6 (x86_64)<br>• Oracle Linux 7 (x86_64) | **Kindly update to fixed version** |

## FORTINET

| TECHNOLOGIES | ADVISORIES | AFFECTED PRODUCTS | RECOMMENDATION |
|---|---|---|---|
| FortiADC | **FortiADC - command injection in web interface** | • FortiADC version 7.0.0 through 7.0.1<br>• FortiADC version 6.2.0 through 6.2.3<br>• FortiADC version 5.4.0 through 5.4.5<br>• FortiADC all versions 6.1<br>• FortiADC all versions 6.0 | **Kindly update to fixed version** |

SECURITY ADVISORY