NETWORK INTELLIGENCE

The Digital Security Company

Feb 2023, Edition 1.0

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- DarkCloud stealer malware attacks surge with widespread spam campaigns by threat actors
- High-severity flaws in Citrix Workspace, Virtual Apps and Desktops
- Vulnerabilities in Google Chrome browser might allow hackers to steal banking details
- Pre-auth double-free vulnerability in OpenSSH server

Also Inside

Security Patch Advisory

Critical High Low

Date: February 27, 2023

DarkCloud stealer malware attacks surge with widespread spam campaigns by threat actors

RECOMMENDATIONS

1. Block the threat indicators at their respective controls.
2. Ensure Microsoft Windows Workstations, Microsoft Exchange Server and Microsoft IIS Server are updated with the latest security patches.
3. Ensure anti-virus and endpoint detection products are up to date with the latest signatures.
4. Refrain from opening untrusted links and email attachments without first verifying their authenticity.
5. Educate employees in terms of protecting themselves from threats like phishing/untrusted URLs.
6. Avoid downloading files from unknown websites.
7. Turn on the automatic software update feature on your computer, mobile, and other connected devices.
8. Use strong passwords and enforce multi-factor authentication wherever possible.
9. Enable Data Loss Prevention (DLP) Solutions on the employees' systems.
10. Keep all systems and software updated to the latest patched versions.
11. Prior to allowing VPN connections from remote endpoints, ensure that posture checking is configured to enforce a baseline set of security controls.
12. Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs.
13. Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.

INTRODUCTION

- DarkCloud is an information stealer malware that collects sensitive information from a victim's computer or mobile device.
- It was first discovered by researchers in 2022, and since then, there has been an increase in its prevalence worldwide.
- DarkCloud Stealer has a multi-stage process, and the final payload is written in Visual Basic.
- It can exfiltrate stolen data via different methods, including SMTP, Telegram, Web Panel, and FTP.
- The malware was found to be sold on a cybercrime forum as a program known as "DarkCloud Stealer Builder," which allows users to tailor the payload of the stealer as per their requirements.
- DarkCloud Stealer can target a range of applications, including browsers and email clients, and it spreads through various spam campaigns.
- The initial file delivered through the spam campaign is a .Net binary that acts as a dropper and creates a task scheduler entry for persistence.
- The payload "credentials.exe" is a 32-bit .NET executable that is identified as a DarkCloud Stealer and gathers confidential information from multiple applications installed on the targeted system and sends it to the Command and Control (C&C).

SECURITY ADVISORY

Date: February 27, 2023

DarkCloud stealer malware attacks surge with widespread spam campaigns by threat actors

HASH (SHA-256)

HASHES	DETECTED BY ANTIVIRUS					
	Symantec	TrendMicro	McAfee	Sophos	Microsoft	SentinelOne
5d060254a6d7eb2cdb2031e29891cb95206757a28fe0d51569eb9f7f55637ac6	NO	YES	YES	YES	YES	NO
79b13d9a52d466a606c37b8f12b2ef7af4e9b53a911b70427c07cb73adb504a1	NO	YES	YES	YES	YES	NO
2e60ed90aa6cefa60cc4cd968213549ddf578dcf6968d8c66366d09c7108ef56	YES	YES	YES	YES	YES	YES
9bb43e190685f86937e09673de3243cbe1971ecf0eab9b75e09d0de96e9764cb	YES	YES	YES	YES	YES	YES
413c9fcea027f89b9d8905ca6ae96cc099b8886fb3916876a4029e92d56fcb9b	YES	YES	YES	NO	YES	YES
e342802bd53191559af2a23b2d11412a8fe60dc3a50e5efa1fade7067c305f55	YES	NO	YES	YES	YES	YES
51247a58f41ba112ce31ed44b0a68bc4db8f39763250071fe35957d1e3eaf9cb	YES	YES	YES	YES	YES	YES
33fa272ffd2eac92f2a344718fa9bf678703f8194fcfcbc499ab9fefcdab4cca	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN

REFERENCES

- Sophisticated Malware Employs Multi-Pronged Data Exfiltration

SECURITY ADVISORY

Date: February 20, 2023

High-severity flaws in Citrix Workspace, Virtual Apps and Desktops

BUSINESS IMPACT

Successful exploitation of the vulnerabilities allows a local attacker to escalate privileges, take control of the affected system, stealthily exfiltrate data, disable security software and plant further malware for disruptive attacks.

RECOMMENDATIONS

1. Kindly update Citrix Workspace (for Linux and Windows), Virtual Apps and Desktops to the latest versions.

INTRODUCTION

Citrix has released fixes to address high-severity vulnerabilities (CVE-2023-24486, CVE-2023-24484, CVE-2023-24485, and CVE-2023-24483) in Citrix Workspace Apps, Virtual Apps and Desktops.

CVE-2023-24486 exists in the Citrix Workspace app for Linux due to an improper access control issue. A malicious user needs access to a system where another user is utilizing a vulnerable version of the Citrix Workspace App for Linux to exploit the bug. Successful exploitation enables a malicious local user to gain access to the Citrix Virtual Apps and Desktops session of another user who is using the same computer from which the ICA session is launched.

CVE-2023-24484 & CVE-2023-24485 exist in the Citrix Workspace app for Windows due to improper access control issues. A malicious user needs access to a system where a vulnerable version of the Citrix Workspace App for Windows is later installed or uninstalled by a SYSTEM process (e.g. SCCM) to exploit the bug. Successful exploitation enables a malicious local user to perform operations as SYSTEM on the computer running Citrix Workspace app.

CVE-2023-24483 exists in Citrix Virtual Apps and Desktops due to improper privilege management issues. To exploit the bug, the attacker needs local access to Windows VDA as a standard Windows user. Successful exploitation enables a local malicious user to elevate the privilege level to NT AUTHORITY\SYSTEM on Citrix Virtual Apps and Desktops Windows VDA.

AFFECTED PRODUCTS

- Citrix Workspace app for Linux before 2302
- Citrix Workspace App for Windows before 2212
- Citrix Workspace App for Windows 2203 LTSR before CU2
- Citrix Workspace App for Windows 1912 LTSR before CU7 Hotfix 2 (19.12.7002)
- Citrix Virtual Apps and Desktops versions before 2212
- Citrix Virtual Apps and Desktops 2203 LTSR before CU2
- Citrix Virtual Apps and Desktops 1912 LTSR before CU6

REFERENCES

- Citrix fixes severe flaws in Workspace, Virtual Apps and Desktops
- Citrix Releases Security Updates for Workspace Apps, Virtual Apps and Desktops

SECURITY ADVISORY

Date: February 16, 2023

Vulnerabilities in Google Chrome browser might allow hackers to steal banking details

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 15 security fixes.

The vulnerabilities are tracked as CVE-2023-0696, CVE-2023-0697, CVE-2023- 0698, CVE-2023-0699, CVE-2023-0700, CVE-2023-0701, CVE-2023-0702, CVE2023-0703, CVE-2023-0704 and CVE-2023-0705.

These vulnerabilities exist in Google Chrome for Desktop due to:

- Type Confusion in V8, Data Transfer, DevTools
- Inappropriate implementation in Full screen mode, Download
- Out of bounds read in WebRTC
- Use after free in GPU
- Heap buffer overflow in WebUI
- Insufficient policy enforcement in DevTools

Cert-In is warning Google Chrome usersthat these vulnerabilities could enable attackers to steal sensitive information such as banking details, date of birth, address and more.

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 110.0.5481.77 (Mac and Linux) and 110.0.5481.77/.78 (Windows).

REFERENCES

- Stable Channel Update for Desktop
- Indian government issues 'high' risk warning, hackers may steal your banking details
- Google Chrome users, here's why government want you to update your browser right now

SECURITY ADVISORY

Date: February 8, 2023

Pre-auth double-free vulnerability in OpenSSH server

BUSINESS IMPACT

Successful exploitation of the vulnerability allows a remote attacker to potentially execute arbitrary code on the target system

INTRODUCTION

OpenSSH has addressed multiple security issues, including a pre-authentication double-free vulnerability (tracked as CVE-2023-25136) with the release of version 9.2.

The vulnerability exists due to a boundary error within the sshd(8) daemon. A remote non-authenticated attacker can send specially crafted data to the application, trigger a double-free error and execute arbitrary code on the target system.

The exploitation of this vulnerability has limitations as double free occurs "in the unprivileged pre-auth process that is subject to chroot (2) and is further sandboxed on most major platforms".

RECOMMENDATIONS

1. Users are recommended to update to OpenSSH 9.2

AFFECTED PRODUCTS

OpenSSH Server 9.1

REFERENCES

- OpenSSH addressed a new pre-auth double free vulnerability
- CVE-2023-25136: Pre-Auth Double Free Vulnerability in OpenSSH Server 9.1

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

6th Feb 2023 – 12th Feb 2023
TRAC-ID: NII23.02.0.2

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-5810-3: Git vulnerabilities	• Ubuntu 16.04 ESM	Kindly update to fixed version
Ubuntu Linux	USN-5835-5: Nova vulnerability	• Ubuntu 18.04 LTS	Kindly update to fixed version

SUSE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
SUSE Linux	SUSE-SU2023:0374-1	• SUSE Linux Enterprise Server 12-SP5	Kindly update to fixed version
SUSE Linux	SUSE-SU2023:0373-1	• SUSE Manager Server 4.3	Kindly update to fixed version

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

6th Feb 2023 – 12th Feb 2023
TRAC-ID: NII23.02.0.2

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2023-12104	• Oracle Linux 6 (i386) • Oracle Linux 6 (x86_64)	**Kindly update to fixed version**
Oracle Linux	ELSA-2023- 12103	• Oracle Linux 6 (i386) • Oracle Linux 6 (x86_64)	**Kindly update to fixed version**

REDHAT

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Red Hat Jboss Data Grid	**RHSA-2023:0713**	• Red Hat JBoss Data Grid Text-Only Advisories x86_64	**Kindly update to fixed version**

SECURITY ADVISORY