NETWORK INTELLIGENCE

The Digital Security Company

August 2022, Edition 1.0

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- Linux Kernel flaw DirtyCred allow local attackers to gain root privileges
- Zero-day vulnerabilities in Apple iPhones, iPads and macOS
- Privilege escalation bugs in Zoom Client for Meetings let hackers gain root access on macOS
- Remote Code Execution & Memory Leak Vulnerabilities in Adobe Acrobat & Acrobat Reader

Also Inside

Security Patch Advisory

Critical High Low

Date: August 23, 2022

Linux Kernel flaw DirtyCred allow local attackers to gain root privileges

BUSINESS IMPACT

Successful exploitation of the vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel and execute arbitrary code in the context of root.

RECOMMENDATIONS

1. Update Linux kernel to latest versions.

2. Isolate privileged credentials from unprivileged ones using virtual memory to prevent cross-cache attacks.

3. Ensure Linux servers and workstations are updated with latest security patches.

INTRODUCTION

Researchers discovered an eight-year-old flaw dubbed DirtyCred in the Linux kernel. DirtyCred is a kernel exploitation concept that swaps unprivileged kernel credentials with privileged ones to escalate privilege. The DirtyCred vulnerability is tracked as CVE-2022-2588. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.

Swapping Linux Kernel Credentials entails three steps:
1. Free an in-use unprivileged credential with the vulnerability
2. Allocate privileged credentials in the freed memory slot
3. Operate as a privileged user

The vulnerability exists due to a double-free error within the network packet scheduler implementation in the route4_change() function in the Linux kernel when removing all references to a route filter before freeing it. A local privileged attacker can run a specially crafted program to crash the kernel or execute arbitrary code, possibly leading to a local privilege escalation issue.

CVSS score: 8.8
The vulnerability can be mitigated by those users who do not rely on cls_route, by adding 'install cls_route /bin/true' to their modprobe.conf or modprobe.d configs, in case it's built as a module.

AFFECTED PRODUCTS

The vulnerability impacts all Linux Kernel versions.

REFERENCES

- 8-year-old Linux Kernel flaw DirtyCred is nasty as Dirty Pipe
- Linux Kernel route4_change Double Free Privilege Escalation Vulnerability

SECURITY ADVISORY

Date: August 18, 2022

Zero-day vulnerabilities in Apple iPhones, iPads and macOS

BUSINESS IMPACT

Successful exploitation of the vulnerabilities allows a remote attacker to trigger out-of-bounds write errors, escalate privileges and execute arbitrary code, break into the operating system and gain broad access to the user's sensitive data.

RECOMMENDATIONS

1. Kindly update macOS, iPadOS, and iOS to the latest version.

INTRODUCTION

Apple has released fixes to address two zero-day vulnerabilities actively exploited in attacks. The vulnerabilities are tracked as CVE-2022-32894 and CVE-2022-32893 were found in WebKit (the browser engine that powers Safari and other apps) and the kernel (the core of the operating system). The two flaws affect iOS, iPadOS and macOS Monterey.

An out-of-bounds write issue (CVE-2022-32894) exists due to a boundary error within the OS kernel component. A local application can trigger an out-ofbounds write error and execute arbitrary code on the system with kernel privileges.

An out-of-bounds write issue (CVE-2022-32893) exists due to a boundary error in WebKit when processing maliciously crafted web content. A remote attacker can create a specially crafted website, trick the victim into opening it, trigger an out-of-bounds write and execute arbitrary code on the target system.

AFFECTED PRODUCTS

- Macs running macOS Monterey
- iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7thgeneration)

REFERENCES

- Apple security updates fix 2 zero-days used to hack iPhones, Macs
- About the security content of macOS Monterey 12.5.1
- About the security content of iOS 15.6.1 and iPadOS 15.6.1

SECURITY ADVISORY

Date: August 18, 2022

Privilege escalation bugs in Zoom Client for Meetings let hackers gain root access on macOS

BUSINESS IMPACT

Successful exploitation of the vulnerabilities allows a local low-privileged attacker to escalate privileges to “superuser” or “root” — allowing them to add, remove, or modify any files on the machine and plant further malware for disruptive operations.

RECOMMENDATIONS

1. Kindly update Zoom Client for Meetings for MacOS to the latest version.

INTRODUCTION

Zoom has released updates to address local privilege escalation flaws in Zoom Client for Meetings for MacOS. The vulnerabilities are tracked as CVE-2022-28757, CVE-2022-28756 & CVE-2022-28751.

The CVE-2022-28757 (CVSS Score: 8.8) and CVE-2022-28756 (CVSS Score: 8.8) bugs exist in Zoom Client for Meetings for MacOS in the auto-update process. The attacker can target the vulnerable installer for the Zoom application, which needs a password for installation/uninstall but doesn’t require a password for auto-updates. A local low-privileged user could exploit this security flaw in the auto-update process to install a malicious update package and escalate their privileges to root.

The CVE-2022-28751 (CVSS Score: 8.8) bug exists in Zoom Client for Meetings for MacOS in the package signature validation during the update process. The vulnerability exists due to an improper checking method in the updater function when given any file with the same name as Zoom’s signing certificate. So, a local, unprivileged attacker could substitute any malware program and run it by the updater with elevated privilege.

AFFECTED PRODUCTS

- Zoom Client for Meetings for macOS (Standard and for IT Admin) starting version 5.7.3 and before version 5.11.6
- Zoom Client for Meetings for MacOS (Standard and for IT Admin) before version 5.11.3

REFERENCES

- Zoom fixed two flaws in macOS App that were disclosed at DEF CON
- The Zoom installer let a researcher hack his way to root access on macOS

SECURITY ADVISORY

Date: August 11, 2022

Remote Code Execution & Memory Leak Vulnerabilities in Adobe Acrobat & Acrobat Reader

BUSINESS IMPACT

Successful exploitation of these vulnerabilities could allow the attacker to cause memory leaks, execute arbitrary code, and compromise the vulnerable system.

RECOMMENDATIONS

1. Ensure Adobe Acrobat and Reader for Windows and macOS is updated with latest security patches.

The latest product versions are available to end users via one of the following methods:

- Users can update their product installations manually by choosing Help > Check for Updates.
- •The products will update automatically, without requiring user intervention, when updates are detected.
- The full Acrobat Reader installer can be downloaded from the Acrobat Reader Download Center.

For IT administrators (managed environments):

- Refer to the specific release note version for links to installers.
- Install updates via your preferred methodology, such as AIP-GPO, bootstrapper, SCUP/SCCM (Windows), or on macOS, Apple Remote Desktop and SSH.

INTRODUCTION

Adobe has released security updates to address multiple Critical and High Severity vulnerabilities in Adobe Acrobat and Reader for Windows and macOS.

The vulnerabilities are tracked as CVE-2022-35665, CVE-2022-35666, CVE-2022-35667, CVE-2022-35668, CVE-2022-35670, CVE-2022-35671 and CVE-2022-35678.

These vulnerabilities exist in Adobe Acrobat and Acrobat Reader due to Use after Free errors, Improper Input Validation, Out of-bounds Write and Read errors. A remote attacker could exploit these vulnerabilities by sending a specially crafted PDF file to the targeted system and convincing the user to open a crafted document.

AFFECTED PRODUCTS

- Acrobat DC and Acrobat Reader DC (Continuous) versions 22.002.20169 and earlier for Windows & MacOS.
- Acrobat 2020 and Acrobat Reader 2020 (Classic 2020) versions 20.005.30362 and earlier for Windows & MacOS.
- Acrobat 2017 and Acrobat Reader 2017 (Classic 2017) versions 17.012.30249 and earlier for Windows & MacOS.

REFERENCES

- Security update available for Adobe Acrobat and Reader | APSB22-39

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

08th Aug 2022 – 14th Aug 2022
TRAC-ID: NII22.08.0.3

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-5568-1: WebKitGTK vulnerabilities	• Ubuntu 22.04 LTS • Ubuntu 20.04 LTS	Kindly update to fixed version
Ubuntu Linux	USN-5569-1: Unbound vulnerabilities	• Ubuntu 22.04 LTS • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS	Kindly update to fixed version

REDHAT

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Red Hat Enterprise Linux	RHSA-2022:6043	• Red Hat Enterprise Linux for x86_64 9 x86_64 • Red Hat Enterprise Linux for IBM z Systems 9 s390x	Kindly update to fixed version
Red Hat Enterprise Linux	RHSA-2022:6024	• Red Hat Enterprise Linux for x86_64 9 x86_64 • Red Hat Enterprise Linux for x86_64 8 x86_64	Kindly update to fixed version

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

08th Aug 2022 – 14th Aug 2022
TRAC-ID: NII22.08.0.3

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2022-5937	• Oracle Linux 7 (x86_64)	Kindly update to fixed version
Oracle Linux	ELSA-2022-5942	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	Kindly update to fixed version

CENTOS

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
CentOS Linux	CESA-2022:5937	• CentOS 7 (x86_64)	Kindly update to fixed version