NETWORK INTELLIGENCE
The Digital Security Company

July 2023, Edition

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- New Apple zero-day bug (CVE-2023-38606) actively exploited in attacks
- CVE-2023-33308: Critical RCE bug in FortiOS & FortiProxy
- New Apple zero-day bug exploited in attacks to hack into iPhones, Macs & iPads
- New SQL injection vulnerabilities in MOVEit Transfer

Also Inside

Security Patch Advisory

Critical High Low

Date: July 26, 2023

New Apple zero-day bug (CVE-2023-38606) actively exploited in attacks

BUSINESS IMPACT

Successful exploitation of the vulnerabilities enables remote attackers to break out of the Web Content sandbox, gain access to sensitive information, achieve arbitrary code execution on vulnerable devices and silently implant spyware or inject surveillance-related malware.

INTRODUCTION

On July 24, Apple released security updates to fix multiple flaws in iOS, iPadOS, macOS, tvOS, watchOS, and Safari.

The updates included fixes for iOS zero-day (CVE-2023-38606) that was exploited in a campaign known as Operation Triangulation. CVE-2023-38606 resides in the kernel that permits a malicious app to modify sensitive kernel state potentially.

CVE-2023-38606 marks the third zero-day from Operation Triangulation attacks that Apple has patched this year. Other zero-days (i.e. CVE-2023-32434 and CVE-2023-32435) exploited in Operation Triangulation attacks were fixed by Apple in June.

Also, Apple has re-released its Rapid Security Response (RSR) updates for the CVE-2023-37450 flaw in iOS and macOS after fixing browsing issues on certain websites caused by the first RSR issued by the company.

RECOMMENDATIONS

1. Update iOS and iPadOS to version 16.6 or above.

2. Update macOS Ventura to version 13.4.1 (a) or above.

3. Update Safari to version 16.5.2 or above.

LESSON LEARNED

- CVE-2023-38606: iPhone 8 and later, iPad Pro (all models), iPad Air 3rd generation and later, iPad 5th generation and later, and iPad mini 5th generation and later running iOS & iPadOS versions before 16.6
- CVE-2023-37450: iOS v16.5.1, iPadOS v16.5.1, macOS Ventura v13.4.1 and Safari versions before 16.5.2

REFERENCES

- Apple addressed a new actively exploited zero-day tracked as CVE2023-38606
- Apple ships that recent “Rapid Response” spyware patch to everyone, fixes a second zero-day

SECURITY ADVISORY

Date: July 13, 2023

CVE-2023-33308: Critical RCE bug in FortiOS & FortiProxy

BUSINESS IMPACT

Successful exploitation of the vulnerability allows an unauthenticated, remote attacker to bypass the authentication process, execute arbitrary code or commands via specifically crafted requests, gain internal network access and deploy further malware for disruptive operations.

INTRODUCTION

On July 11, Fortinet disclosed a critical flaw (CVE-2023-33308) affecting FortiOS & FortiProxy and urged organizations to apply the patches immediately. The bug is more likely to be exploited in targeted hacking campaigns & malware attacks.

CVE-2023-33308 (CVSS Score: 9.8) is a Stack-based buffer overflow issue when processing specially crafted packets in devices running FortiOS & FortiProxy.

A remote unauthenticated attacker can send specially crafted packets to the device having proxy policies or firewall policies with proxy mode alongside SSL deep packet inspection, trigger a stack-based buffer overflow and execute arbitrary code on the target system.

WORKAROUND

If admins are unable to apply the new firmware immediately, Fortinet recommends disabling HTTP/2 support on SSL inspection profiles used by proxy policies or firewall policies with proxy mode.

AFFECTED PRODUCTS

- FortiOS version 7.2.0 through 7.2.3
- FortiOS version 7.0.0 through 7.0.10
- FortiProxy version 7.2.0 through 7.2.2
- FortiProxy version 7.0.0 through 7.0.9

RECOMMENDATIONS

1. Please upgrade FortiProxy to version 7.2.3 or above and 7.0.10 or above.

2. Please upgrade FortiOS to version 7.4.0 or above, 7.2.4 or above and 7.0.11 or above.

REFERENCES

Fortinet warns of critical RCE flaw in FortiOS, FortiProxy devices

FortiOS/FortiProxy - Proxy mode with deep inspection - Stack-based buffer overflow

Fortinet Releases Security Update for FortiOS and FortiProxy

SECURITY ADVISORY

Date: July 11, 2023

New Apple zero-day bug exploited in attacks to hack into iPhones, Macs & iPads

BUSINESS IMPACT

Successful exploitation of the vulnerabilities enables remote attackers to break out of the Web Content sandbox, gain access to sensitive information, achieve arbitrary code execution on vulnerable devices and silently implant spyware or inject surveillance-related malware.

INTRODUCTION

On July 10, as part of Rapid Security Response (RSR) updates, Apple addressed a new zero-day vulnerability (CVE-2023-37450) actively exploited in attacks in the wild to hack into iPhones, Macs, and iPads.

CVE-2023-37450 flaw exists in the WebKit browser engine. Apple stated that it had addressed the security issue with improved checks.

A remote attacker can trick the victim into visiting specially crafted web content and gain arbitrary code execution on targeted devices.

RECOMMENDATIONS

1. Update iOS and iPadOS to version 16.5.1 (a) or above.

2. Update macOS Ventura to version 13.4.1 (a) or above.

AFFECTED PRODUCTS

- iOS v16.5.1
- iPadOS v16.5.1
- macOS Ventura v13.4.1

REFERENCES

Apple releases emergency update to fix zero-day exploited in attacks

Apple Issues Urgent Patch for Zero-Day Flaw Targeting iOS, iPadOS, macOS, and Safari

SECURITY ADVISORY

Date: July 7, 2023

New SQL injection vulnerabilities in MOVEit Transfer

BUSINESS IMPACT

Successful exploitation of the vulnerabilities may allow a remote attacker to gain unauthorized access to the MOVEit Transfer database, execute arbitrary code in the context of the moveitsvc user and shut down the MOVEit Transfer application

RECOMMENDATIONS

1. Ensure to update MOVEit Transfer to versions 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), 2023.0.4 (15.0.4).

BUSINESS IMPACT

On July 06, Progress addressed three new vulnerabilities (CVE-2023-36934, CVE-2023-36932 and CVE-2023-36933) as part of the July 2023 Service Pack.

CVE-2023-36934 flaw exists within the human.aspx endpoint. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that can trigger the execution of SQL queries composed from a user-supplied string to execute code in the context of the moveitsvc user. CVSS SCORE: 9.8

CVE-2023-36932 exists due to multiple SQL injection vulnerabilities in the MOVEit Transfer web application. A crafted request can result in unauthorized access, modification and disclosure of MOVEit database content.

CVE-2023-36933 allows an attacker to invoke a method that results in an unhandled exception and triggers unexpected termination of the MOVEit Transfer application.

AFFECTED PRODUCTS

- The vulnerabilities affect multiple MOVEit Transfer versions, including 12.1.10 and previous versions, 13.0.8 and earlier, 13.1.6 and earlier, 14.0.6 and older, 14.1.7 and older, and 15.0.3 and earlier.

REFERENCES

Another Critical Unauthenticated SQLi Flaw Discovered in MOVEit Transfer Software 2. MOVEit Transfer 2020.1 (12.1) Service Pack (July 2023)

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

10th July 2023 – 16th July 2023
TRAC-ID: NII23.07.0.3

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-6213-1: Ghostscript vulnerability	• Ubuntu 23.04 • Ubuntu 22.10 • Ubuntu 22.04 LTS • Ubuntu 20.04 LTS	Kindly update to fixed version
Ubuntu Linux	USN-6214-1: Thunderbird vulnerabilities	• Ubuntu 23.04 • Ubuntu 22.10 • Ubuntu 22.04 LTS • Ubuntu 20.04 LTS	Kindly update to fixed version

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2023-12590 - Unbreakable Enterprise kernel-container security update	• Oracle Linux 7 (x86_64)	Kindly update to fixed version
Oracle Linux	ELSA-2023-12591 - Unbreakable Enterprise kernel-container security update	• Oracle Linux 8 (x86_64)	Kindly update to fixed version

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

10th July 2023 – 16th July 2023
TRAC-ID: NII23.07.0.3

FORTINET

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
FortiOS	FortiOS - Existing websocket connection persists after deleting API admin	• FortiOS version 7.2.0 through 7.2.4 • FortiOS 7.0 all versions	**Kindly update to fixed version**
FortiOS & FortiProxy	FortiOS/FortiProxy - Proxy mode with deep inspection - Stack-based buffer overflow	• FortiOS version 7.2.0 through 7.2.3 • FortiOS version 7.0.0 through 7.0.10 • FortiProxy version 7.2.0 through 7.2.2 • FortiProxy version 7.0.0 through 7.0.9	**Kindly update to fixed version**

BITDEFENDER

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Bitdefender Engines	**Out of Bounds Memory Corruption Issue in CEVA Engine (VA11010)**	• Bitdefender Engines version 7.94791 and lower	**Kindly update to fixed version**

SECURITY ADVISORY