UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0302

APPLE FIXES TWO ZERO-DAY VULNERABILITIES

DATE ISSUED: 10th April 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

Security researchers with Google Threat Analysis Group and Amnesty International Security Lab discovered two zero-day vulnerabilities being actively exploited as part of an exploit chain to compromise iPhones, Macs, and iPads.

BREAKDOWN

The first zero-day vulnerability, tracked as CVE-2023-28206, is an IOSurfaceAccelerator that enables an attacker to execute arbitrary code with kernel privileges on targeted devices by using a malicious app. This could lead to the corruption of data, a crash, or code execution. The second zero-day vulnerability tracked as CVE-2023-28205 is a Webkit browser engine that powers Safari and other apps. It could allow attackers to control code execution within Webkit, giving them the ability to read/write files. WebKit bugs are often exploited when someone visits a malicious domain in their browser (or via in-app services). It's not uncommon for bad actors to find vulnerabilities that target WebKit to break into the device's operating system and the user's private data. WebKit bugs can be "chained" to other vulnerabilities to break through multiple layers of a device's defences. Apple addressed the zero-days in iOS 15.7.5, iPadOS 15.7.5, macOS Monterey 12.6.5, and macOS Big Sur 11.7.6 by improving input validation and memory management.

REMEDIATION STEPS

- Install the security updates as soon as possible to mitigate potential threats.
- Implement a Patch Management policy and process to reduce the attack surface introduced by unpatched software.
- Leverage Next-Generation Antivirus (NGAV) to block zero-day malware, which was previously unknown.
- Monitor network traffic: Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.

REFERENCES & RESOURCES

The Bleeping Computer	https://www.bleepingcomputer.com/news/apple/apple-fixes-recently-disclosed-zero-days-on-older-iphones-and-ipads/
Apple	https://support.apple.com/en-us/HT201222