Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apple Addresses Zero-Day Flaws Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
September 25, 2023	A1	TA2023385

Summary

First Seen: September 21, 2023
Affected Products: iPhone, iOS, iPadOS, macOS, watchOS, and Safari
Affected Platform: macOS
Malware: Predator
Impact: Apple addressed three zero-day vulnerabilities used in an iPhone exploit chain to deliver the Predator spyware. The vulnerabilities involved were CVE-2023-41991, CVE-2023-41992, and CVE-2023-41993. These vulnerabilities enabled attackers to bypass certificate validation, escalate privileges, and execute remote code on the targeted devices by using specially crafted web content.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-41991	Apple Signature Bypass Vulnerability	iPhone, iOS, iPadOS, macOS, watchOS, and Safari	✓	✓	✓
CVE-2023-41992	Apple Privilege Escalation Vulnerability	iPhone, iOS, iPadOS, macOS, watchOS, and Safari	✓	✓	✓
CVE-2023-41993	Apple Arbitrary Code Execution Vulnerability	iPhone, iOS, iPadOS, macOS, watchOS, and Safari	✓	✓	✓

Vulnerability Details

#1

Apple addressed three zero-day vulnerabilities, identified as CVE-2023-41991, CVE-2023-41992, and CVE-2023-41993. These vulnerabilities had the potential to allow a malicious actor to bypass certificate validation, elevate privileges, and achieve remote code execution on targeted devices. This could be accomplished by manipulating specially crafted web content during the exploitation process.

#2

CVE-2023-41991, arises from the inadequate verification of cryptographic signatures within the Security component. An attacker could potentially exploit this vulnerability, deceiving victim to install malicious applications, thereby evading the signature validation process.

#3 CVE-2023-41992 denotes a kernel-level security vulnerability where a local attacker may have the capability to escalate their privileges. This vulnerability arises from the lack of adequate validation of user-supplied input within the operating system kernel. As a consequence, a local application could potentially execute arbitrary code on the system with elevated privileges.

#4 The vulnerability, CVE-2023-41993, enables an attacker to trigger memory corruption and execute arbitrary code on the target device. This is achieved by enticing victims to visit a specially crafted website. The root cause of this vulnerability lies in a boundary error that occurs during the processing of HTML content within WebKit.

#5 These vulnerabilities were employed in an iPhone exploit chain, facilitating the deployment of the "Predator" spyware. The target of this attack was identified as a former member of the Egyptian parliament, and the infection was executed via network injection. All HTTP requests were automatically redirected to a malicious website, resulting in the installation of Cytrox's Predator spyware on the victim's phone. The traffic redirection was occurring at a device located on the border of Vodafone Egypt's network.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-41991	iPhone, iOS 17.0 21A327 - 17.0 21A331, iPadOS 17.0, macOS 13.0 22A380 - 13.5.2 22G91, watchOS 10.0, and Safari	cpe:2.3:o:apple:ipad_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	CWE-295
CVE-2023-41992	iPhone, iOS 17.0 21A327 - 17.0 21A331, iPadOS 17.0, macOS 13.0 22A380 - 13.5.2 22G91, watchOS 10.0, and Safari	cpe:2.3:o:apple:ipad_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	CWE-754
CVE-2023-41993	iPhone, iOS 17.0 21A327 - 17.0 21A331, iPadOS 17.0, macOS 13.0 22A380 - 13.5.2 22G91, watchOS 10.0, and Safari	cpe:2.3:o:apple:ipad_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	CWE-754

Recommendations

Apply Patch: Install the security patch provided by Apple to address the CVE-2023-41991, CVE-2023-41992, and CVE-2023-41993 vulnerabilities. These patches shall close the security gap that allows attackers to exploit the vulnerability.

Adhere to Mobile Security Principles:

- Only download apps from the official Apple App Store.
- Revisit app permissions and Only grant access to the information or features that an app truly needs to function.
- Be cautious about clicking on links in emails or text messages, especially if you didn't expect to receive them. Verify the sender's legitimacy before taking any action.
- Avoid opening unsolicited web links, and always verify if a link offers HTTPS protection and ensures a secure HTTPS connection

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0042** Resource Development	**TA0004** Privilege Escalation	**TA0001** Initial Access
T1203 Exploitation for Client Execution	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1068** Exploitation for Privilege Escalation
T1189 Drive-by Compromise	**T1566** Phishing		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	almal-news[.]com, chat-support[.]support, cibeg[.]online, notifications-sec[.]com, wa-info[.]com, whatssapp[.]co, wts-app[.]info

Patch Link

https://support.apple.com/en-us/HT213927

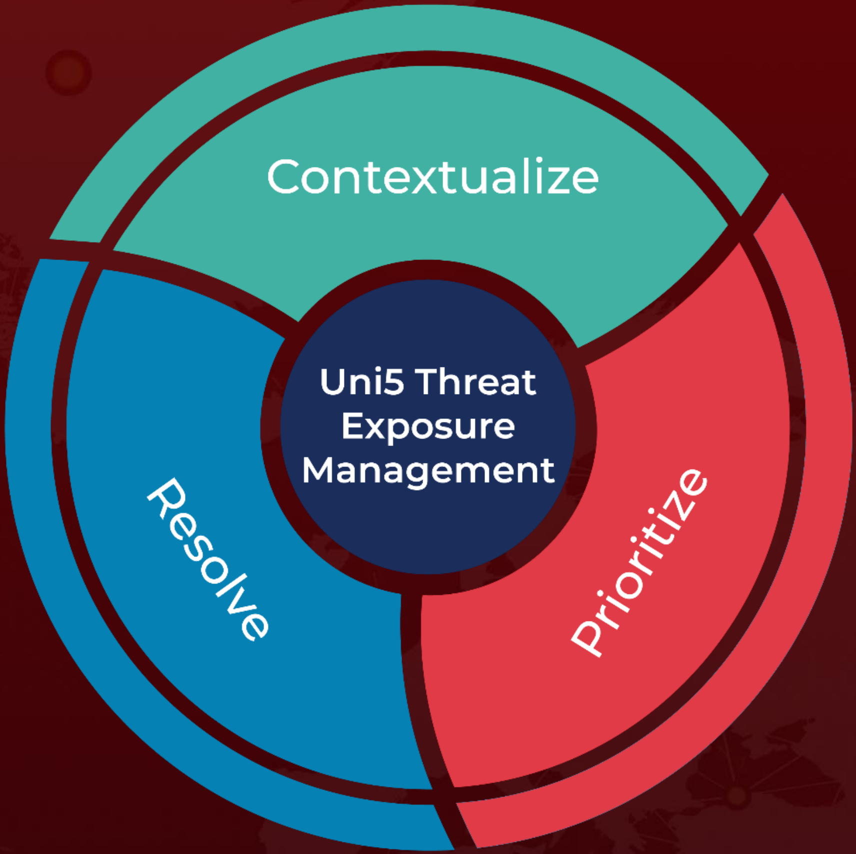
References

https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 25, 2023 • 6:40 AM

More at www.hivepro.com