Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

New 'HM-Surf' Vulnerability Could Expose MacOS Data

Date of Publication	Admiralty Code	TA Number
October 21, 2024	A1	TA2024403

Summary

First Seen: September 16, 2024
Affected Product: macOS Sequoia 15
Malware: Adload
Impact: The macOS vulnerability known as HM Surf (CVE-2024-44133), allows attackers to bypass the Transparency, Consent, and Control (TCC) framework, granting unauthorized access to sensitive data like the camera and microphone. Active exploitation has been linked to the adware family Adload. Apple has released security updates to address this issue. Users are advised to install updates promptly and exercise caution with app permissions.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-44133	HM Surf	macOS Sequoia 15	✗	✗	✓

Vulnerability Details

#1 A recently discovered macOS vulnerability, known as HM Surf and tracked as CVE-2024-44133, poses a significant risk by allowing attackers to bypass the operating system's Transparency, Consent, and Control (TCC) framework. This flaw enables unauthorized access to sensitive user data, including the camera, microphone, browsing history, and location services.

#2 The exploitation of HM Surf involves several steps. Attackers can bypass TCC protections specifically targeting the Safari browser directory. By modifying a configuration file within this directory, they can gain access to sensitive information without user consent.

#3 The process typically involves changing the home directory of the current user using macOS utilities, allowing attackers to alter sensitive files (like PerSitePreferences.db) in the Safari directory. After making these changes, they revert the home directory back to its original state, enabling Safari to utilize these modified files.

#4 Once access is gained, attackers could capture snapshots or entire camera streams, record audio through the microphone, or retrieve location data. Notably, this method leverages specific entitlements that only Apple's applications possess, making third-party browsers like Chrome or Firefox immune to this particular exploit.

#5 Security researchers has reported signs of active exploitation related to this vulnerability, particularly linked to Adload, a known adware family targeting macOS systems. While it remains unclear if Adload is directly exploiting HM Surf, suspicious activities have been detected that warrant immediate attention from users.

#6 In response to the discovery of HM Surf, Apple released security updates as part of macOS Sequoia on September 16, 2024. These updates address the vulnerability by removing the exploitable code and enhancing protections for configuration files against unauthorized modifications.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-44133	macOS Sequoia versions before 15.0	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	CWE-284

Recommendations

Install Security Updates Promptly: Regularly check for and apply all available security patches from Apple. Timely updates help protect your system from known vulnerabilities like HM Surf. Staying current is crucial for maintaining device security.

Enable Automatic Updates: Turn on automatic updates to ensure your macOS receives the latest security enhancements without delay. This feature helps safeguard your system against emerging threats. It reduces the risk of overlooking critical updates.

Review App Permissions: Be cautious when granting permissions to applications, especially those requesting access to sensitive data. Regularly review which apps have access to your camera, microphone, and location services. Limiting permissions can help protect your privacy.

Monitor for Suspicious Activity: Keep an eye on your system for any unusual behavior or unauthorized access attempts. If you notice anything suspicious, report it to Apple Support immediately. Early detection can mitigate potential damage from exploitation.

Use Trusted Software: Download applications only from reputable sources, such as the Mac App Store or verified developers. Avoid third-party sites that may host malicious software. Using trusted software minimizes the risk of malware infections.

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	**TA0042** Resource Development	**TA0007** Discovery	**TA0002** Execution
TA0011 Command and Control	**TA0005** Defense Evasion	**T1071.001** Web Protocols	**T1071** Application Layer Protocol
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1068** Exploitation for Privilege Escalation	**T1588.005** Exploits
T1082 System Information Discovery	**T1033** System Owner/User Discovery	**T1059.002** AppleScript	**T1059.004** Unix Shell
T1140 Deobfuscate/Decode Files or Information	**T1222** File and Directory Permissions Modification	**T1222.002** Linux and Mac File and Directory Permissions Modification	

Patch Details

Upgrades to macOS Sequoia version 15.0 or later.

Links:
https://support.apple.com/en-us/121238

https://support.apple.com/en-us/108382

References

https://support.apple.com/en-us/121238

https://www.microsoft.com/en-us/security/blog/2024/10/17/new-macos-vulnerability-hm-surf-could-lead-to-unauthorized-data-access/

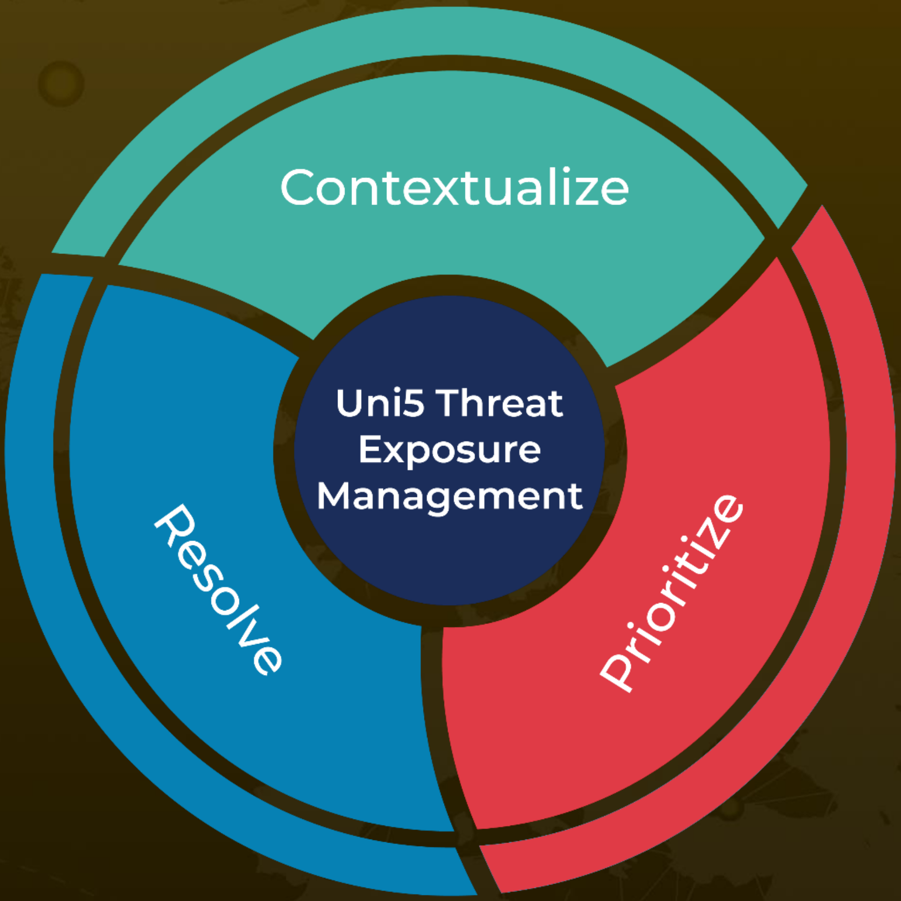
https://github.com/yo-yo-yo-jbo/hm-surf/blob/main/README.md

https://www.hivepro.com/adload-malware-persists-on-mac-systems-with-new-proxy-payload/

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

October 21, 2024 • 6:30 AM

More at www.hivepro.com