Hive Pro

Threat Level

Amber

HiveForce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

# Apple Discovers Three New Vulnerabilities in macOS Ventura 13.2

| Date of Publication | Admiralty Code | TA Number |
|---|---|---|
| February 27, 2023 | A1 | TA2023103 |

# Summary

**First Seen:** February 20, 2023
**Affected Product:** Apple macOS Ventura
**Impact:** Remote code execution; Race condition; Privilege escalation

## CVEs

| CVE | NAME | PATCH |
|---|---|---|
| CVE-2023-23520 | Race Condition vulnerability in crash reporter component | ✓ |
| CVE-2023-23530 | Remote code execution vulnerability in Foundation component | ✓ |
| CVE-2023-23531 | Privilege escalation vulnerability in Foundation component | ✓ |

# Vulnerability Details

Apple has updated its macOS Ventura 13.2 advisories to include three new vulnerabilities. One of them is a race condition affecting the crash reporter component, which can allow an attacker to read arbitrary files as root. The other two security holes impact the 'foundation' component, allowing an attacker to execute arbitrary code out of its sandbox or with certain elevated privileges. Exploiting these vulnerabilities can lead to code execution and access to sensitive data.

## Vulnerability

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2023-23520 | macOS: 13.0 22A380 - 13.1 22C65 | cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* | CWE-362 |
| CVE-2023-23530 | macOS: 13.0 22A380 - 13.1 22C65 | cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* | CWE-94 |
| CVE-2023-23531 | macOS: 13.0 22A380 - 13.1 22C65 | cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* | CWE-94 |

# Recommendations

**Security Leaders**

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

**Security Engineers**

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Patch Details' on the following pages.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0002<br>Execution | TA0005<br>Defense Evasion | TA0009<br>Collection | TA0040<br>Impact |
| T1036<br>Masquerading | T1070<br>Indicator Removal | T1070.004<br>File Deletion | T1059<br>Command and Scripting Interpreter |
| T1055<br>Process Injection | T1005<br>Data from Local System | T1213<br>Data from Information Repositories | T1486<br>Data Encrypted for Impact |
| T1561<br>Disk Wipe | | | |

## Patch Details

Update to version macOS Ventura 13.2

## References

https://support.apple.com/en-us/HT213605

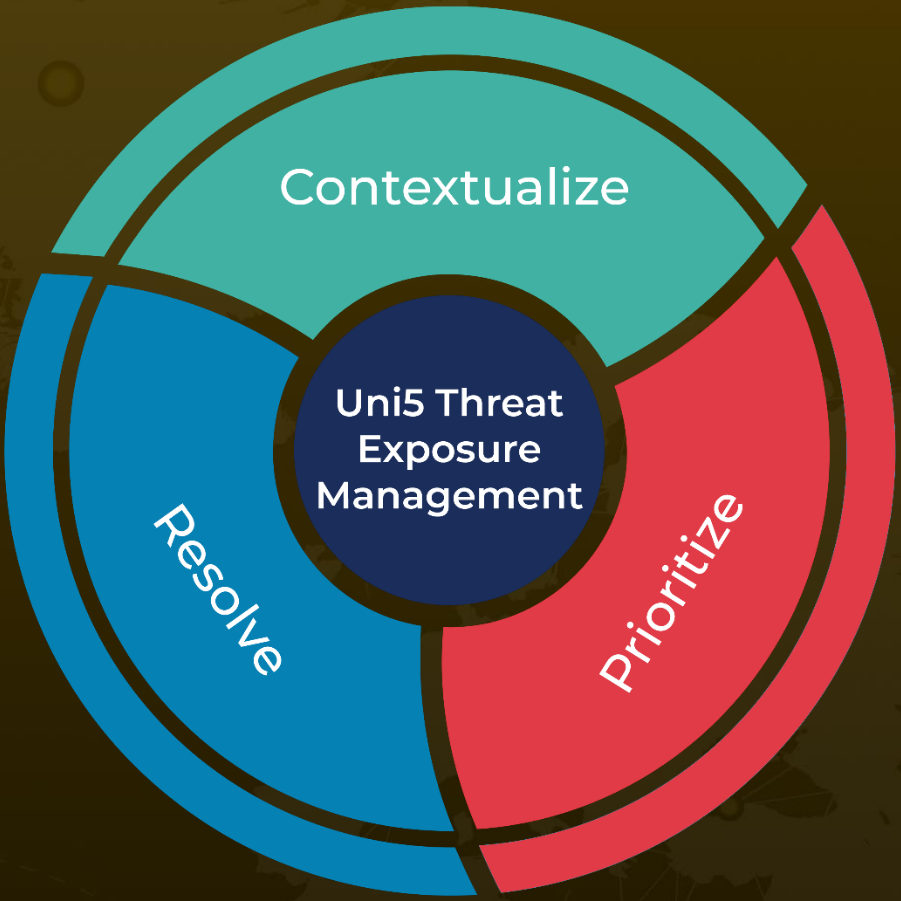
https://www.trellix.com/en-us/about/newsroom/stories/research/trellix-advanced-research-center-discovers-a-new-privilege-escalation-bug-class-on-macos-and-ios.html

https://www.securityweek.com/apple-updates-advisories-as-security-firm-discloses-new-class-of-vulnerabilities/

# 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

**February 27, 2023 • 1:20 AM**

More at www.hivepro.com