National Cyber Security Centre

2408020119-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerabilities in Apple Mobile & Smart Devices Operating Systems

Friday 2nd August, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-07-29T23:15:00
Vendor: Apple
Products: iOS, iPadOS, macOS, watchOS, visionOS, tvOS
CVE IDs:

- CVE-2024-27826 |CVSS3.0 Score[1]: n/a | EPSS[2]: 0.176760000
- CVE-2024-40788 |CVSS3.0 Score n/a | EPSS: 0.176760000

CVE-2024-27826 is flaw in the kernel that could allow an attacker execute arbitrary code with kernel privileges. CVE-2024-40788 could allow a local attacker cause an unexpected system shutdown.

For up to date EPSS score, click here:

- https://api.first.org/data/v1/epss?cve=CVE-2024-27826
- https://api.first.org/data/v1/epss?cve=CVE-2024-40788

Products Affected

CVE-2024-27862

- iOS prior to version 17.5
- iPadOS prior to version 17.5
- watchOS prior to version 10.5
- visionOS prior to version 1.3
- tvOS prior to version 17.5
- macOS prior to versions
  - Ventura 13.6.8
  - Sonoma 14.5
  - Monterey 12.7.6

CVE-2024-40788

- iOS prior to version 17.6
- iPadOS prior to version 17.6
- watchOS prior to version 10.6
- visionOS prior to version 1.3
- macOS prior to versions
  - Ventura 13.6.8
  - Sonoma 14.6
  - Monterey 12.7.6

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins

Impact

- **CVE-2024-27862**
  - **Common Weakness Enumeration (CWE)[3]:** An app may be able to execute arbitrary code with kernel privileges
  - **Present in CISA Known Exploited Vulnerability(KEV)[4] catalog:** NO
  - **Used by Ransomware Operators:** Not Known.

- **CVE-2024-40788**
  - **Common Weakness Enumeration (CWE)** A local attacker may be able to cause unexpected system shutdown A type confusion issue was addressed with improved memory handling.
  - **Present in CISA Known Exploited Vulnerability(KEV) catalog:** NO
  - **Used by Ransomware Operators:** Not Known.

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Apple.

Additional recommendations and mitigation's for CVE-2024-27826 and CVE-2024-40788 can be found in the respective links below:

- iOS 17.5 and iPadOS 17.5: https://support.apple.com/en-us/HT214101
- tvOS 17.5: https://support.apple.com/en-us/HT214102
- watchOS 10.5: https://support.apple.com/en-us/HT214104
- macOS Sonoma 14.5: https://support.apple.com/en-us/HT214106
- iOS 16.7.9 and iPadOS 16.7.9: https://support.apple.com/en-us/HT214116
- iOS 17.6 and iPadOS 17.6: https://support.apple.com/en-us/HT214117
- macOS Monterey 12.7.6: https://support.apple.com/en-us/HT214118
- macOS Sonoma 14.6: https://support.apple.com/en-us/HT214119
- macOS Ventura 13.6.8: https://support.apple.com/en-us/HT214120
- tvOS 17.6: https://support.apple.com/en-us/HT214122
- visionOS 1.3: https://support.apple.com/en-us/HT214123
- watchOS 10.6: https://support.apple.com/en-us/HT214124

[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 K7X4,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre