National Cyber Security Centre

2309080190-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Actively exploited Apple OS vulnerabilities - Update

Tuesday 12th September, 2023

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.

Revision History

Revision	Date	Author(s)	Description
1.0	8 Sept 2023	CSIRT-IE	Initial advisory.
1.1	12 Sept 2023	CSIRT-IE	Updated products affected.

Description

Apple has released security updates that address two new vulnerabilities CVE-2023-41064 and CVE-2023-41061 that affect ImageIO and Wallet respectively. Exploitation of these vulnerabilities could result in arbitrary code execution.

At time of reporting Apple is aware of a report that these vulnerabilities may have been actively exploited in the wild.

Products Affected

- macOS Monterey 12.6.8 and below
- macOS Big Sur 11.7.9 and below
- macOS Ventura 13.5.1 and below
- iOS 16.6.0 and below
- iPadOS 16.6.0 and below
- watchOS 9.6.1 and below

Impact

Exploitation of these vulnerabilities could result in arbitrary code execution.

Recommendations

The NCSC strongly advises affected organisations to implement the available patches issued by Apple. It is also recommended that individuals who might be at heightened risk due to their identity or activities follow Apple's Lockdown Mode guide.

Further information can be found here:

- Apple iOS and iPadOS Security Update
- Apple macOS Ventura Security Update
- Apple watchOS Security Update
- About Lockdown Mode

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
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie