National Cyber Security Centre

2109140847-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Apple iMessage vulnerability being exploited
2021-09-14

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, 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.*

Threat Type	The NCSC has been made aware that attackers are exploiting a vulnerability known as “ForcedEntry” that affects iOS, macOS, and watchOS. It allows a remote attacker to gain access to a device without any user interaction. The vulnerability has been exploited since at least February 2021. Apple has released an update to resolve this vulnerability. Apple have issued updates for the vulnerability here, the vulnerability allows maliciously crafted documents to execute commands when opened on vulnerable devices.
Products Affected	This vulnerability affects. • All iPhones with iOS versions prior to 14.8 • All Mac computers with operating system versions prior to OSX Big Sur 11.6 • All Apple Watches prior to watchOS 7.6.2.
Impact	Remote Code Execution - compromised systems, data loss.
Recommendations	The NCSC recommends that affected users update the Apple products as soon as possible.

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