

Vulnerability Assessment

How to Determine Vulnerability Severity

Remote Code Execution? Yes

CVE-2021-30860 is classified as a remote code execution (RCE) vulnerability because attackers could execute malicious code remotely via specially crafted PDFs sent through Apple iMessage. The exploit allowed attackers to compromise a device without physically accessing it or requiring the victim to open a file or click a link.

Local Access Required? No

The ForcedEntry exploit was a zero-click vulnerability, meaning attackers didn't need local access to the device. The exploit could be delivered remotely through iMessage and executed automatically when processed by the Apple device.

Authentication Required? No

Attackers didn't need valid credentials or authentication to exploit the vulnerability. The exploit targeted how Apple devices processed malicious image and PDF content in iMessage.

Proof of Concept Available? Yes

Citizen Lab researchers documented and analyzed the exploit chain after identifying it on a victim's device. The research provided technical evidence showing how the exploit worked and how the vulnerability was exploited in real-world attacks.

Exploit Actively Being Used in the Wild? Yes

According to Citizen Lab, the ForcedEntry exploit was actively used in targeted spyware campaigns involving the NSO Group's Pegasus spyware platform. The exploit was identified on devices belonging to activists and other targeted individuals.

Vendor Confirmed? Yes

Apple confirmed the vulnerability and issued security advisories for CVE-2021-30860. Apple acknowledged that the vulnerability was actively exploited before the patch was released.

Patch Available? Yes

Apple released security updates addressing CVE-2021-30860 for iOS, iPadOS, macOS, and watchOS. Users were advised to update their devices immediately to reduce the risk of compromise.

CVSS 3.1 Breakdown for CVE-2021-30860

- **Attack Vector: Network**
The vulnerability could be exploited remotely over the network through Apple iMessage.
- **Attack Complexity: Low**
The exploit didn't require special conditions or advanced preparation once the malicious message was delivered.
- **Privileges Required: None**
Attackers didn't need authorized access before exploitation.
- **User Interaction: None**
The exploit was zero-click and required no action from the victim.
- **Scope: Changed**
Successful exploitation allowed the attacker to impact resources beyond the vulnerable component's original security scope.
- **Confidentiality: High**
Attackers could gain access to sensitive information stored on the device.
- **Integrity: High**
Attackers could modify or manipulate data on the compromised device.
- **Availability: High**
Attackers could disrupt system operations or fully compromise device functionality.

References

Marczak, B., Scott-Railton, J., Razzak, B. A., Aljizawi, N., Anstis, S., Berdan, K., & Deibert, R. (2021, September 13). *FORCEDENTRY NSO: Group iMessage Zero-Click Exploit Captured in the Wild*. Citizen Lab. <https://citizenlab.ca/research/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/>

National Institute of Standards and Technology. (n.d.). *CVSS v3.1 calculator*. National Vulnerability Database. <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

National Institute of Standards and Technology. (n.d.). *CVE-2021-30860 detail*. National Vulnerability Database. <https://nvd.nist.gov/vuln/detail/CVE-2021-30860>