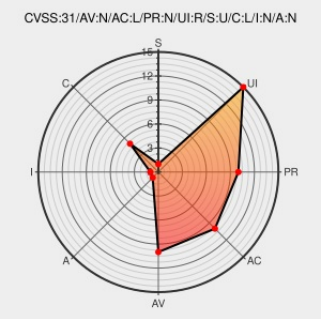
CVE-2020-9857

Published on: 10/27/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:15 PM UTC

CVE-2020-9857

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mac Os X from Apple contain the following vulnerability:

An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.5, Security Update 2020-003 Mojave, Security Update 2020-003 High Sierra. A malicious website may be able to exfiltrate autofilled data in Safari.

CVE-2020-9857 has been assigned by product-security@apple.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Apple** - **macOS** version **< 10.15**

CVSS3 Score: 4.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
About the security content of macOS Catalina 10.15.5, Security Update 2020-003 Mojave,	Release Notes	MISC

Security Update 2020-003 High Sierra - Apple Support	Vendor Advisory support.apple.com text/html	support.apple.com/en-us/HT211170

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→