



CVE-2018-4441

Published on: 04/03/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:16 PM UTC

CVE-2018-4441

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Icloud](#) from [Apple](#) contain the following vulnerability:

A memory corruption issue was addressed with improved memory handling. This issue affected versions prior to iOS 12.1.1, tvOS 12.1.1, watchOS 5.1.2, Safari 12.0.2, iTunes 12.9.2 for Windows, iCloud for Windows 7.9.

CVE-2018-4441 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
About the security content of watchOS 5.1.2 - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/kb/HT209343
About the security content of iOS 12.1.1 - Apple Support	Vendor Advisory	MISC support.apple.com/kb/HT209340

support.apple.com
text/html

About the security content of Safari 12.0.2 - Apple Support

Vendor Advisory
support.apple.com
text/html

🍏 MISC support.apple.com/kb/HT209344

About the security content of tvOS 12.1.1 - Apple Support

Vendor Advisory
support.apple.com
text/html

🍏 MISC support.apple.com/kb/HT209342

About the security content of iCloud for Windows 7.9 - Apple Support

Vendor Advisory
support.apple.com
text/html

🍏 MISC support.apple.com/kb/HT209346

About the security content of iTunes 12.9.2 for Windows - Apple Support

Vendor Advisory
support.apple.com
text/html

🍏 MISC support.apple.com/kb/HT209345

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

A WebKit exploit using CVE-2018-4441 to obtain RCE on PS4 6.20.

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Icloud	All	All	All	All
Application	Apple	Icloud	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Application	Apple	Itunes	All	All	All	All
Application	Apple	Itunes	All	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Apple	Safari	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All

System						
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
cpe:2.3:a:apple:icloud:*:*:*:*:*:*:						
cpe:2.3:a:apple:icloud:*:*:*:*:*:*:						
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:						
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:						
cpe:2.3:a:apple:itunes:*:*:*:*:*:*:						
cpe:2.3:a:apple:itunes:*:*:*:*:*:*:						
cpe:2.3:a:apple:safari:*:*:*:*:*:*:						
cpe:2.3:a:apple:safari:*:*:*:*:*:*:						
cpe:2.3:o:apple:tvos:*:*:*:*:*:*:						
cpe:2.3:o:apple:tvos:*:*:*:*:*:*:						
cpe:2.3:o:apple:watchos:*:*:*:*:*:*:						
cpe:2.3:o:apple:watchos:*:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE