JQUERY - CVE-2012-6708

PUBLISHED: MARCH 17, 2020 | LAST UPDATE: AUGUST 16, 2021

SUMMARY

In June 2012, a Cross-site Scripting (XSS) vulnerability in jQuery was disclosed [1] and subsequently published in January 2018. The following vulnerability reported in the disclosure may affect the management plane of ACOS devices and is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2012-6708	CVSS 3.0	6.1 Medium	js-jquery: XSS via improper selector detection [2]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to this vulnerability and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

Customers using affected ACOS releases can overcome vulnerability exposures by updating to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no ACOS release update is currently available.

Releases Affected			Releases Resolved or Unaffected
4.1.4	–	4.1.4-GR1-P1	4.1.4-GR1-P2, 5.0.0
4.1.2	–	4.1.2-P5	4.1.2-P6
4.1.1	–	4.1.1-P11	4.1.1-P12
4.1.100	–	4.1.100-P6	4.1.100-P7
4.1.0	–	4.1.0-P12	4.1.0-P13
3.2.4	–	3.2.4-P4	3.2.4-P5, 3.2.5, 5.0.1-TPS

WORKAROUNDS AND MITIGATIONS

None

SOFTWARE UPDATES

Software updates that address these vulnerabilities are or will be published at the following URL:

http://www.a10networks.com/support/axseries/software-downloads

VULNERABILITY DETAILS

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2012-6708	jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common..

RELATED LINKS

Ref #	General Link
[1]	Cross-site Scripting (XSS) Affecting jquery package, versions >=1.7.1 <1.9.0

[2] NIST NVD, CVE-2012-6708

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2020-03-17	Initial Publication
2.0	2021-08-16	Add resolved releases for 4.1.4-GR1, 3.2.4, 3.2.5-TPS