WAF - SQL INJECTION ATTACK (SQLIA) VULNERABILITY

PUBLISHED: JULY 18, 2018 | LAST UPDATE: JULY 23, 2018

SUMMARY

A remote attacker could send specially-crafted SQL statements, which could be passed through by the ACOS Web Application Firewall (WAF) rather than being dropped per configured rules. This could allow a remote attacker to conduct an SQL injection attack on targeted systems. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	A10-2017-0008 [(a)]	CVSS 3.0	7.4 High	WAF: SQL Injection Attack (SQLIA) Vulnerability

[(a)] A10 Networks, Inc. assigned identifier.

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities 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
4.1.2	–	4.1.2-P3	4.1.2-P4
4.1.1	–	4.1.1-P7	4.1.1-P8
4.1.0	–	4.1.0-P10	4.1.0-P11
2.7.2	–	2.7.2-P11	2.7.2-P12
2.7.1-GR1	–	2.7.1-GR1-Px	2.7.2-P12, 4.1.0-P11, 4.1.1-P8, 4.1.2-P4, 4.1.4

WORKAROUNDS AND MITIGATIONS

Include the following ACOS aFleX command as an effective mitigation for this vulnerability, in lieu of upgrading to a resolved release indicated above and recognizing that this workaround may have a negative impact on throughput and performance of the ACOS system.

```
WAF::rule sqlia-check HTTP_REQUEST_DATA {REQUEST_COOKIES_NAMES REQUEST_COOKIES ARGS_NAMES ARGS}
{URL_DECODE_UNICODE LOWERCASE} {@POLICY sqlia_defs} {
        log "field [WAF::matched var] name [WAF::matched name] may contain SQL: [WAF::matched match 0]"
        WAF::action deny
}
```

`WAF::rule` is an undocumented aFleX command, the format of which is:

```
WAF::rule name event variable-list transformation-list match action
```

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
A10-2017-0008	SQL injection vulnerability in ACOS Web Application Firewall (WAF) allows attackers to execute arbitrary SQL commands via unspecified vectors on protected systems.

RELATED LINKS

None

ACKNOWLEDGEMENTS

A10 Networks, Inc would like to thank Luca Profico from Quantum Leap Srl for reporting this vulnerability.

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-18	Initial Publication
2.0	2018-07-23	Added acknowledgement.