# TCP/IP - CVE-2018-5391 (FRAGMENTSMACK)

PUBLISHED: AUGUST 19, 2018 | LAST UPDATE: SEPTEMBER 10, 2018

## SUMMARY

In August 2018, US CERT released a vulnerability note [1] regarding a security exposure in IPv4 fragment processing of Linux kernels. The following vulnerabilities reported in that US CERT notice that affect the management plane of ACOS systems are addressed in this document.

IPv4 processing in the dataplane of ACOS systems is not exposed to this vulnerability.

| Item # | Vulnerability ID | Score Source | Score | Summary |
|---|---|---|---|---|
| 1 | CVE-2018-5391 | CVSS 3.0 | 7.8 High | IP fragments with random offsets allow a remote denial of service (FragmentSmack) [2] |

## 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 |
|---|---|---|---|
| 4.1.4 | – | 4.1.4-P2 | 4.1.4-P3 |
| 4.1.2 | – | 4.1.2-P4 | 4.1.2-P5 |
| 4.1.1 | – | 4.1.1-P8 | 4.1.1-P9 |
| 4.1.0 | – | 4.1.0-P11 | 4.1.0-P12 |
| 3.2.2 | – | 3.2.2-P5 | 3.2.2-P6, 3.2.3 |

## WORKAROUNDS AND MITIGATIONS

Common security best practices in the industry for network appliance management and control planes can enhance protection against remote malicious attacks. Limit the exploitable attack surface for critical, infrastructure, networking equipment through the use of access lists or firewall filters to and from only trusted, administrative networks or hosts.

This consideration can be applied for UDP services of the ACOS management plane; such as LDAPS (external authentication), NTP (time synchronization), DNS (name resolution requests), and TFTP (ACOS file import operations).

## 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-2018-5391 | A flaw named FragmentSmack was found in the way the Linux kernel handled reassembly of fragmented IPv4 and IPv6 packets. A remote attacker could use this flaw to trigger time and calculation expensive fragment reassembly algorithm by sending specially crafted packets which could lead to a CPU saturation and hence a denial of service on the system.<br><br>A result of the 30 kpps attack on the physical system with Intel(R) Xeon(R) D-1587@1.70GHz CPUs and 32 cores in total may look like a complete saturation of a core |

## RELATED LINKS

| Ref # | General Link |
|---|---|
| [1] | US CERT, Vulnerability Note VU#641765 |
| [2] | NIST NVD, CVE-2018-5391 |

## ACKNOWLEDGEMENTS

None

## MODIFICATION HISTORY

| Revision | Date | Description |
|---|---|---|
| 1.0 | 2018-08-19 | Initial Publication |
| 1.1 | 2018-08-20 | Grammatic correction in Summary section. |
| 2.0 | 2018-08-29 | Updated affected and resolved releases. |
| 3.0 | 2018-09-10 | Updated to confirm ACOS dataplane not exposed to vulnerability. |