EX SERIES - CVE-2017-13704, CVE-2017-14491

PUBLISHED: OCTOBER 9, 2018 | LAST UPDATE: OCTOBER 9, 2018

SUMMARY

In October 2017, vulnerabilities were published for Dnsmasq, a lightweight DNS forwarder. These following vulnerabilities that affect the data-plane DNS services of A10 EX Series products are addressed in this document. End of Life Notices [1] were issued for EX Series products between 2010 and 2015.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2017-13704	CVSS 3.0	7.5 High	dnsmasq: Size parameter overflow via large DNS query [2]
2	CVE-2017-14491	CVSS 3.0	9.8 Critical	dnsmasq: heap overflow in the code responsible for building DNS replies [3]

AFFECTED RELEASES

The table below indicates releases of EX Series software exposed to these vulnerabilities and EX Series software releases that address them. EX Series release families not indicated below are unaffected by these vulnerabilities.

Customers using affected EX Series 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 EX Series release update is currently available.

Releases Affected			Releases Resolved or Unaffected
2.2.0	–	2.2.1	- none -
3.0.0	–	3.0.2	- none -
3.1.0	–	3.1.0 Update 4	- none -
3.2.0	–	3.2.0 Update 2	- none -

WORKAROUNDS AND MITIGATIONS

Apply the following alternate workarounds as mitigations for these vulnerabilities.

1. If all DNS requests/replies that relate to "inbound" traffic are forwarded by the EX system, disable DNS services in the EX system with the following EX configuration operations.

   - Via EX CLI:
     - "no dns enable"

   - Via EX GUI
     - Navigate to Config Mode --> Network --> DNS
     - Click the "Local DNS Server" tab
     - Uncheck the "Enable Local DNS Server" checkbox to disable the DNS Server

2. If the EX DNS service is configured to only resolve domains used by inbound LLB, ensure that the service is not configured to work as a DNS proxy with the following EX configuration operations.

   - Via EX CLI:
     - “no dns enable proxy”
     - Remove all "dns proxy-server xxx" configuration items, if currently configured.
     - Do not add DNS servers with the command “dns proxy-server xxx”

- Via Ex GUI
  - Navigate to Config Mode --> Network --> DNS
  - Click the "Local DNS Server" tab
  - Check the "Enable Local DNS Server" checkbox to enable DNS Server
  - Uncheck the "Enable DNS Proxy" checkbox to disable the DNS Proxy
  - Navigate to Config Mode --> Network --> Domain Based Proxy
  - Delete all domain proxy server entries configured

3. Use DNS Servers under the company's control that are deemed to be trusted (safe) and not a potential source of malicious, crafted DNS responses such as involved with this vulnerability.

SOFTWARE UPDATES

Software updates for EX Series products may be found at the following URL:

https://www.a10networks.com/support/exseries/downloads

VULNERABILITY DETAILS

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

Vulnerability ID	Description
CVE-2017-13704	In dnsmasq before 2.78, if the DNS packet size does not match the expected size, the size parameter in a memset call gets a negative value. As it is an unsigned value, memset ends up writing up to 0xffffffff zero's (0xffffffffffffffff in 64 bit platforms), making dnsmasq crash.
CVE-2017-14491	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response.

RELATED LINKS

Ref #	General Link
[1]	A10 End of Sales
[2]	NIST NVD, CVE-2017-13704
[3]	NIST NVD, CVE-2017-14491

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-10-09	Initial Publication