ICMP - TIMESTAMP RESPONSE, CVE-1999-0524

PUBLISHED: AUGUST 8, 2017 | LAST UPDATE: OCTOBER 17, 2019

SUMMARY

A vulnerability scan of the ACOS management interface indicated the presence of responses to ICMP timestamp requests. The information in these responses could be leveraged in other exploits of the ACOS system. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	generic-icmp-timestamp	Rapid7	1 Moderate	ICMP timestamp response [1]
2	CVE-1999-0524	CVSS 2.0	0.0 Low	ICMP timestamp response [2]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities and ACOS releases that address these issues or are otherwise unaffected by them.

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-P1
4.1.1	–	4.1.1-P2	4.1.1-P3
4.1.100	–	4.1.100-P5-SP1	4.1.100-P6
4.1.0	–	4.1.0-P8	4.1.0-P9
3.1.0-P1	–	3.2.1-P1	3.2.2-P1
2.8.2	–	2.8.2-P8	4.1.2-P1
2.7.2	–	2.7.2-P7	4.1.0-P9, 4.1.1-P3
2.7.1	–	2.7.1-GR1-P1	4.1.0-P9, 4.1.1-P3
2.6.1-GR1	–	2.6.1-GR1-P16	4.1.0-P9, 4.1.1-P3

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.

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
generic-icmp-timestamp	The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services. In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.
CVE-1999-0524	ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.

RELATED LINKS

Ref #	General Link
[1]	Rapid7: ICMP timestamp response
[2]	NIST NVD, CVE-1999-0524

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-08-08	Initial Publication
2.0	2019-10-17	Added 4.1.100 release family.