STRONGSWAN- CVE-2021-41991, CVE-2021-45079

PUBLISHED: OCTOBER 31, 2022 | LAST UPDATE: OCTOBER 31, 2022

Summary

In October 2021 and January 2022, Strongswan.org disclosed [1, 2] vulnerabilities that could lead to denial-of-service attacks or bypass EAP authentication. These vulnerabilities could affect IPsec services in the management or data plane of ACOS devices and are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2021-41991	CVSSv3	7.5 High	strongswan: integer overflow when replacing certificates in cache [3]
2	CVE-2021-45079	CVSSv3	9.1 Critical	strongswan: Incorrect Handling of Early EAP-Success Messages [4]

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
5.0.0	–	5.2.1-P5	5.2.1-P6
4.1.4-GR1	–	4.1.4-GR1-P11	4.1.4-GR1-P12

Workarounds and Mitigations

None

Software Updates

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

https://support.a10networks.com/

Vulnerability Details

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

Vulnerability ID	Description
CVE-2021-41991	The in-memory certificate cache in strongSwan before 5.9.4 has a remote integer overflow upon receiving many requests with different certificates to fill the cache and later trigger the replacement of cache entries. The code attempts to select a less-often-used cache entry by means of a random number generator, but this is not done correctly. Remote code execution might be a slight possibility.
CVE-2021-45079	In strongSwan before 5.9.5, a malicious responder can send an EAP-Success message too early without actually authenticating the client and (in the case of EAP methods with mutual authentication and EAP-only authentication for IKEv2) even without server authentication.

Related Links

Ref #	General Link
[1]	strongSwan Vulnerability (CVE-2021-41991)
[2]	strongSwan Vulnerability (CVE-2021-45079)
[3]	NIST NVD, CVE-2021-41991
[4]	NIST NVD, CVE-2021-45079

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2022-10-31	Initial Publication

This document is provided on an "AS IS" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability, non-infringement or fitness for a particular use. Your use of the information in this document or materials linked from this document is at your own risk. A10 Networks, Inc. reserves the right to change or update the information in this document at any time.