RADIUS PROTOCOL- CVE-2024-3596

PUBLISHED: MARCH 20, 2025 | LAST UPDATE: MARCH 20, 2025

Summary

A RADIUS Protocol vulnerability was published on July 9, 2024. RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can forge an authentication response in cases where a Message-Authenticator attribute is not required or enforced. This issue arises from a cryptographically insecure integrity check using MD5, enabling attackers to spoof UDP-based RADIUS response packets. This could allow an attacker to undermine the fundamental security mechanisms of RADIUS-based authentication systems.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2024-3596	CVSSv3	9.0 Critical	RADIUS Protocol: forgery attack [1]

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
6.0.0	–	6.0.5	6.0.6
5.2.1	–	5.2.1-P11	5.2.1-P12
4.1.4	–	4.1.4-GR1-P14	4.1.4-GR1-P14-SP1

Workarounds and Mitigations

This vulnerability involves malicious or Man-In-The-Middle RADIUS servers for exploitation. Manage and configure ACOS devices for RADIUS authentication operations only with trusted RADIUS servers on trusted communication channels.

For ACOS 6.0.6, 5.2.1-P12 or 4.1.4-GR1-P14-SP1 and newer:

Enable the message authenticator attribute verification using the following config command:

```
ACOS(config)# radius-server message-authenticator-verify-enable
```

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-2024-3596	RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature.

Related Links

Ref #	General Link
[1]	https://nvd.nist.gov/vuln/detail/CVE-2024-3596

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2025-03-20	Initial Publication