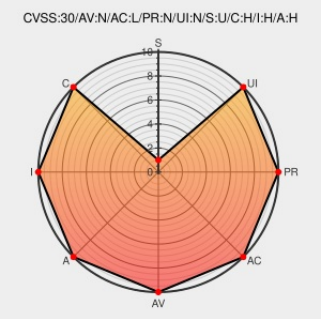
CVE-2016-9125

Published on: 03/27/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:16 PM UTC

CVE-2016-9125

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Revive Adserver from Revive-adserver contain the following vulnerability:

Revive Adserver before 3.2.3 suffers from session fixation, by allowing arbitrary session identifiers to be forced and, at the same time, by not invalidating the existing session upon a successful authentication. Under some circumstances, that could have been an opportunity for an attacker to steal an authenticated session.

CVE-2016-9125 has been assigned by support@hackerone.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Revive Adserver Security Advisory SA-2016-001 | Revive Adserver	Patch Vendor Advisory www.revive-adserver.com	MISC www.revive-adserver.com/security/revive-sa-2016-001/

	text/html	
Fix h1 reports 93809 and 93813 · revive-adserver/revive-adserver@4910365 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/revive-adserver/revive-adserver/commit/4910365631eabbb208961c36149f41cc8159fb39
HackerOne	Permissions Required hackerone.com text/html	MISC hackerone.com/reports/93809
HackerOne	Permissions Required hackerone.com text/html	MISC hackerone.com/reports/93813

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Revive-adserver	Revive Adserver	All	All	All	All

cpe:2.3:a:revive-adserver:revive_adserver:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→