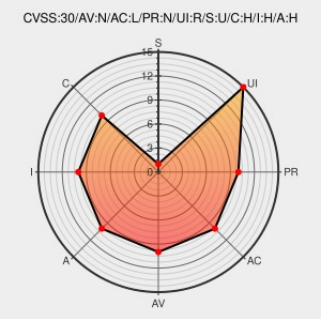
CVE-2016-9127

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

Last Modified on: 03/23/2021 11:27:17 PM UTC

CVE-2016-9127

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 Cross-Site Request Forgery (CSRF). The password recovery form in Revive Adserver is vulnerable to CSRF attacks. This vulnerability could be exploited to send a large number of password recovery emails to the registered users, especially in conjunction with a bug that caused recovery emails to be sent to all the users at once. Both issues have been fixed.

CVE-2016-9127 has been assigned by support@hackerone.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	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	MISC www.revive-adserver.com/security/revive-sa-2016-001/

	www.revive-adserver.com text/html	
HackerOne	Permissions Required hackerone.com text/html	MISC hackerone.com/reports/99452
Fix h1 report 99452 · revive-adserver/revive-adserver@3aaebcc · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/revive-adserver/revive-adserver/commit/3aaebcc765797d2c684e031f2836e0a69d6b7bc2

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→