

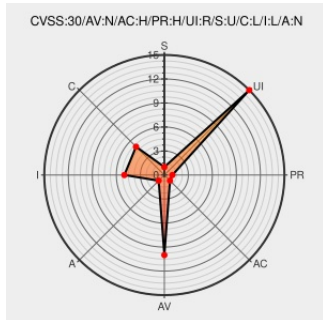


CVE-2016-9471

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

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

CVE-2016-9471

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Revive Adserver](#) from [Revive-adserver](#) contain the following vulnerability:

Revive Adserver before 3.2.5 and 4.0.0 suffers from Special Element Injection. Usernames weren't properly sanitised when creating users on a Revive Adserver instance. Especially, control characters were not filtered, allowing apparently identical usernames to co-exist in the system, due to the fact that such characters are normally ignored when

an HTML page is displayed in a browser. The issue could have therefore been exploited for user spoofing, although elevated privileges are required to create users within Revive Adserver.

CVE-2016-9471 has been assigned by [h1](#) support@hackerone.com to track the vulnerability - currently rated as [LOW](#) severity.

CVSS3 Score: [3.1 - LOW](#)

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

CVSS2 Score: [2.1 - LOW](#)

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
-------------	------	------

Fix h1 report 128181 · revive-adserver/revive-adserver@05b1ece · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/revive-adserver/revive-adserver/commit/05b1eceb
HackerOne	Permissions Required hackerone.com text/html	 MISC hackerone.com/reports/128181
Revive Adserver Security Advisory SA-2016-002	Patch Vendor Advisory www.revive-adserver.com text/html	 MISC www.revive-adserver.com/security/revive-sa-2016-002/

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	4.0.0	All	All	All
Application	Revive-adserver	Revive Adserver	4.0.0	All	All	All
Application	Revive-adserver	Revive Adserver	All	All	All	All
cpe:2.3:a:revive-adserver:revive_adserver:4.0.0:*:*:*:*:*:						
cpe:2.3:a:revive-adserver:revive_adserver:4.0.0:*:*:*:*:*:						
cpe:2.3:a:revive-adserver:revive_adserver:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)