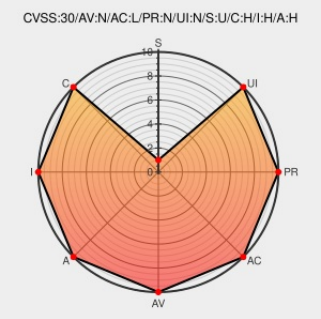
CVE-2019-5434

Published on: 05/06/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:00 PM UTC

CVE-2019-5434

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



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

An attacker could send a specifically crafted payload to the XML-RPC invocation script and trigger the unserialize() call on the "what" parameter in the "openads.spc" RPC method. Such vulnerability could be used to perform various types of attacks, e.g. exploit serialize-related PHP vulnerabilities or PHP object injection. It is possible, although unconfirmed, that the vulnerability has been used by some attackers in order to gain access to some Revive Adserver instances and deliver malware through them to third party websites. This vulnerability was addressed in version 4.2.0.

CVE-2019-5434 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

HackerOne	Third Party Advisory hackerone.com text/html	MISC hackerone.com/reports/512076
Revive Adserver Security Advisory SA-2019-001	Vendor Advisory www.revive-adserver.com text/html	MISC www.revive-adserver.com/security/revive-sa-2019-001/
HackerOne	Third Party Advisory hackerone.com text/html	MISC hackerone.com/reports/542670
Revive Adserver 4.2 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/155559/Revive-Adserver-4.2-Remote-Code-Execution.html

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-sas	Revive Adserver	All	All	All	All
Application	Revive-sas	Revive Adserver	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→