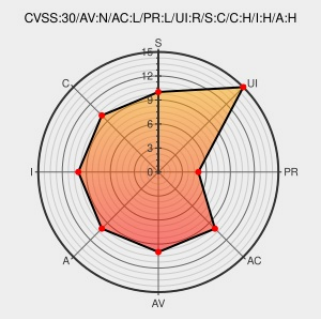
CVE-2017-17055

Published on: 12/06/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:27 PM UTC

CVE-2017-17055

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



Certain versions of Artica Proxy from Articatech contain the following vulnerability:

Artica Web Proxy before 3.06.112911 allows remote attackers to execute arbitrary code as root by conducting a cross-site scripting (XSS) attack involving the username-form-id parameter to freeradius.users.php.

CVE-2017-17055 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 8.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Full Disclosure: Artica Web Proxy v3.06 Remote Code Execution / CVE-2017-17055	Exploit, Mailing List, Third Party Advisory, seclists.org, text/html	FULLDISC 20171201 Artica Web Proxy v3.06 Remote Code Execution / CVE-2017-17055

	Exploit Vendor Advisory hyp3rlinx.altervista.org text/plain	MISC hyp3rlinx.altervista.org/advisories/ARTICA-WEB-PROXY-v3.06-REMOTE-CODE-EXECUTION-CVE-2017-17055.txt
Artica Web Proxy 3.06.112216 Remote Code Execution ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/145183/Artica-Web-Proxy-3.06.112216-Remote-Code-Execution.html
Artica Web Proxy 3.06 - Remote Code Execution - PHP webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 43206

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	Articatech	Artica Proxy	All	All	All	All
Application	Articatech	Artica Proxy	All	All	All	All

cpe:2.3:a:articatech:artica_proxy:*:*:*:*:*:*:*:*:

cpe:2.3:a:articatech:artica_proxy:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→