



CVE-2021-29156

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-29156
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-25 09:15:00 UTC
Updated	2021-03-29 12:17:00 UTC
Description	ForgeRock OpenAM before 13.5.1 allows LDAP injection via the Webfinger protocol. For example, an unauthenticated attacker can inject LDAP queries into the Webfinger protocol response, which can be used to perform a denial of service attack.

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Forgerock	Openam	All	All	All	All

References

Reference	Source	Link
[OPENAM-10135] Classic UI customizations not found due to incorrect defaultOrg format - ForgeRock JIRA	MISC	bugster.forgerock.com
Hidden OAuth attack vectors PortSwigger Research	MISC	portswigger.net
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[731203](#) ForgeRock OpenAM LDAP Injection Vulnerability

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](#)