CVE-2020-27847

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-27847
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-28 11:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	A vulnerability exists in the SAML connector of the github.com/dexidp/dex library used to process SAML Signature Validatic

Risk And Classification

Problem Types: CWE-228

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Dex	All	All	All	All

References

Reference	Source	Link
Critical security issues in XML encoding · Advisory · dexidp/dex · GitHub	MISC	github.com
1907732 – (CVE-2020-27847) CVE-2020-27847 dexidp/dex: authentication bypass in saml authentication	MISC	bugzilla.redhat.com
Coordinated disclosure of XML round-trip vulnerabilities in Go library	MISC	mattermost.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report