CVE-2021-21335

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-21335
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-08 21:15:00 UTC
Updated	2021-03-12 14:21:00 UTC
Description	In the SPNEGO HTTP Authentication Module for nginx (spnego-http-auth-nginx-module) before version 1.1.1 basic Authent

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spnego Http Authentication Module Project	Spnego Http Authentication Module	All	All	All	All
Application	Spnego Http Authentication Module Project	Spnego Http Authentication Module	All	All	All	All

References

Reference
Basic Authentication can be bypassed using a malformed username · Advisory · stnoonan/spnego-http-auth-nginx-module · GitHub
Release Rollup of changes since v1.1 · stnoonan/spnego-http-auth-nginx-module · GitHub
Check basic auth result against != NGX_OK rather than == NGX_DECLINED · stnoonan/spnego-http-auth-nginx-module@a06f9ef · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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