CVE-2022-40735

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

Summary

CVE	CVE-2022-40735
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-14 23:15:00 UTC
Updated	2024-01-11 03:15:00 UTC
Description	The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecess

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Diffie-hellman Key Exchange Project	Diffie-hellman Key Exchange	-	All	All	All

References

Reference	Source	Link
Just a moment...	MISC	www.research
RFC 5114: Additional Diffie-Hellman Groups for Use with IETF Standards	MISC	www.rfc-edito
RFC 4419: Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol	MISC	www.rfc-edito
link.springer.com/content/pdf/10.1007/3-540-68339-9_29.pdf	MISC	link.springer.c
RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)	MISC	www.rfc-edito
D(HE)at Attack | D(HE)at Attack		dheatattack.gi
raw.githubusercontent.com/CVEProject/cvelist/9d7fbbcabd3f44cfedc9e8807757d31ece85a2c6/2...	MISC	raw.githubuse
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf	MISC	nvlpubs.nist.g
Diffie-Hellman short exponent references · GitHub	MISC	gist.github.co
Stop recommending DHE, because of "dheater" vulnerability · Issue #162 · mozilla/ssl-config-generator · GitHub	MISC	github.com
RFC 7919: Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)	MISC	www.rfc-edito
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.

Free CVE JSON API cve.report/api

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