



# CVE-2022-40735

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-40735
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-11-14 23:15:00 UTC
<b>Updated</b>	2024-01-11 03:15:00 UTC
<b>Description</b>	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	<a href="#">www.research</a>
RFC 5114: Additional Diffie-Hellman Groups for Use with IETF Standards	MISC	<a href="#">www.rfc-edito</a>
RFC 4419: Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol	MISC	<a href="#">www.rfc-edito</a>
<a href="#">link.springer.com/content/pdf/10.1007/3-540-68339-9_29.pdf</a>	MISC	<a href="#">link.springer.c</a>
RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)	MISC	<a href="#">www.rfc-edito</a>
D(HE)at Attack   D(HE)at Attack		<a href="#">dheatattack.gi</a>
<a href="#">raw.githubusercontent.com/CVEProject/cvelist/9d7fbbcabd3f44cfedc9e8807757d31ece85a2c6/2...</a>	MISC	<a href="#">raw.githubuse</a>
<a href="#">nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf</a>	MISC	<a href="#">nvlpubs.nist.g</a>
Diffie-Hellman short exponent references · GitHub	MISC	<a href="#">gist.github.cor</a>
Stop recommending DHE, because of "dheater" vulnerability · Issue #162 · mozilla/ssl-config-generator · GitHub	MISC	<a href="#">github.com</a>
RFC 7919: Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)	MISC	<a href="#">www.rfc-edito</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)