# CVE Detail – CVE-2022-40735

The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wiener paper found that "(appropriately) short exponents" can be used when there are adequate subgroup constraints, and these short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-2002-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are not public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability concern because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.78743

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-400: Uncontrolled Resource Consumption

## CAPEC(s)

* CAPEC-147: XML Ping of the Death
* CAPEC-227: Sustained Client Engagement
* CAPEC-492: Regular Expression Exponential Blowup

## ATT&CK Techniques

* T1499: Endpoint Denial of Service

## Used By (Actors/Tools)

* OnionDuke (malware)
* ZxShell (malware)
* Sandworm Team (intrusion-set)

## Affected Products

* cpe:2.3:a:diffie-hellman\_key\_exchange\_project:diffie-hellman\_key\_exchange:-:\*:\*:\*:\*:\*:\*:\*