# CVE Detail – CVE-2002-20001

The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)at or D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.94161

## 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:balasys:dheater:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:siemens:scalance\_w1750d\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_server:11:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_server:12:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_server:15:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_access\_policy\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_firewall\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_web\_application\_firewall:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_analytics:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_acceleration\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_security\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_visibility\_and\_reporting:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_carrier-grade\_nat:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_ddos\_hybrid\_defender:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_domain\_name\_system:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_edge\_gateway:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_fraud\_protection\_service:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_global\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_link\_controller:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_local\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_policy\_enforcement\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_service\_proxy:1.6.0:\*:\*:\*:\*:kubernetes:\*:\*
* cpe:2.3:a:f5:big-ip\_ssl\_orchestrator:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_webaccelerator:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_websafe:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-iq\_centralized\_management:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-iq\_centralized\_management:7.1.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:traffix\_signaling\_delivery\_controller:5.1.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:traffix\_signaling\_delivery\_controller:5.2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:f5:f5os-a:1.3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:f5:f5os-a:1.3.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:f5:f5os-c:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:f5:f5os-c:1.5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:f5:f5os-c:1.5.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:hpe:arubaos-cx:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:hpe:arubaos-cx:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:hpe:arubaos-cx:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:hpe:arubaos-cx:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:stormshield:stormshield\_management\_center:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:stormshield:stormshield\_network\_security:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:stormshield:stormshield\_network\_security:\*:\*:\*:\*:\*:\*:\*:\*