CVE-2002-20001

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2002-20001
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-11 19:15:00 UTC
Updated	2024-01-11 03:15:00 UTC
Description	The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that ar

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Balasys	Dheater	-	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Visibility And Reporting	All	All	All	All
Application	F5	Big-ip Carrier-grade Nat	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All

Application	F5	Big-ip Service Proxy	1.6.0	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Websafe	All	All	All	All
Application	F5	Big-iq Centralized Management	7.1.0	All	All	All
Application	F5	Big-iq Centralized Management	All	All	All	All
Application	F5	F5os-a	1.3.0	All	All	All
Application	F5	F5os-a	1.3.1	All	All	All
Application	F5	F5os-c	1.5.0	All	All	All
Application	F5	F5os-c	1.5.1	All	All	All
Application	F5	F5os-c	All	All	All	All
Application	F5	Traffix Sdc	5.1.0	All	All	All
Application	F5	Traffix Sdc	5.2.0	All	All	All
Application	F5	Traffix Signaling Delivery Controller	5.1.0	All	All	All
Application	F5	Traffix Signaling Delivery Controller	5.2.0	All	All	All
Operating System	Hpe	Arubaos-cx	All	All	All	All
Hardware	Hpe	Aruba Cx 4100i	-	All	All	All
Hardware	Hpe	Aruba Cx 6100	-	All	All	All
Hardware	Hpe	Aruba Cx 6200f	-	All	All	All
Hardware	Hpe	Aruba Cx 6200m	-	All	All	All
Hardware	Hpe	Aruba Cx 6300f	-	All	All	All
Hardware	Hpe	Aruba Cx 6300m	-	All	All	All
Hardware	Hpe	Aruba Cx 6405	-	All	All	All
Hardware	Hpe	Aruba Cx 6410	-	All	All	All
Hardware	Hpe	Aruba Cx 8320	-	All	All	All
Hardware	Hpe	Aruba Cx 8325-32c	-	All	All	All
Hardware	Hpe	Aruba Cx 8325-48y8c	-	All	All	All
Hardware	Hpe	Aruba Cx 8360-12c	-	All	All	All
Hardware	Hpe	Aruba Cx 8360-16y2c	-	All	All	All
Hardware	Hpe	Aruba Cx 8360-24xf2c	-	All	All	All
Hardware	Hpe	Aruba Cx 8360-32y4c	-	All	All	All
Hardware	Hpe	Aruba Cx 8360-48xt4c	-	All	All	All
Hardware	Hpe	Aruba Cx 8360-48y6c	-	All	All	All
Hardware	Hpe	Aruba Cx 8400	-	All	All	All
Hardware	Siemens	Scalance W1750d	-	All	All	All

Operating System	Siemens	Scalance W1750d Firmware	All	All	All	All
Application	Stormshield	Stormshield Management Center	All	All	All	All
Application	Stormshield	Stormshield Network Security	All	All	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Server	15	All	All	All

References

Reference	Source	Link
Security Vulnerability: DHEater aka CVE-2002-20001 | Support | SUSE	MISC	www.suse
D(HE)at Attack / dheater · GitLab	MISC	gitlab.com
GitHub - Balasys/dheater: D(HE)ater is a security tool can perform DoS attack by enforcing the DHE key exchange.	MISC	github.com
Server overload by enforcing DHE key exchange using minimal bandwidth : netsec	MISC	www.redd
Configuring Supported TLS Groups in OpenSSL - OpenSSL Blog	MISC	www.oper
support.f5.com/csp/article/K83120834	MISC	support.f5
dheatattack.com	MISC	dheatattac
D(HE)at Attack | D(HE)at Attack		dheatattac
cert-portal.siemens.com/productcert/pdf/ssa-506569.pdf	CONFIRM	cert-portal
www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-004.txt	MISC	www.arub
Stop recommending DHE, because of "dheater" vulnerability · Issue #162 · mozilla/ssl-config-generator · GitHub	MISC	github.com
ResearchGate	MISC	www.rese
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

376752 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Diffie-Hellman key agreement protocol Vulnerability (K83120834)

591188 Siemens SCALANCE W1750D Multiple Vulnerabilities (ICSA-22-314-10, SSA-506569)

site. This site includes MITRE data granted under the following license.

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