



CVE-2002-0428

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2002-0428
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-08-12 04:00:00 UTC
Updated	2008-09-05 20:28:00 UTC
Description	Check Point FireWall-1 SecuRemote/SecuClient 4.0 and 4.1 allows clients to bypass the "authentication timeout" by modify

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkpoint	Check Point Vpn	1_4.1	All	All	All
Application	Checkpoint	Check Point Vpn	1_4.1_sp1	All	All	All
Application	Checkpoint	Check Point Vpn	1_4.1_sp2	All	All	All
Application	Checkpoint	Check Point Vpn	1_4.1_sp3	All	All	All
Application	Checkpoint	Check Point Vpn	1_4.1_sp4	All	All	All
Application	Checkpoint	Check Point Vpn	1_4.1	All	All	All
Application	Checkpoint	Check Point Vpn	1_4.1_sp1	All	All	All
Application	Checkpoint	Check Point Vpn	1_4.1_sp2	All	All	All
Application	Checkpoint	Check Point Vpn	1_4.1_sp3	All	All	All
Application	Checkpoint	Check Point Vpn	1_4.1_sp4	All	All	All
Application	Checkpoint	Firewall-1	4.0	All	All	All
Application	Checkpoint	Firewall-1	4.0	sp1	All	All
Application	Checkpoint	Firewall-1	4.0	sp2	All	All
Application	Checkpoint	Firewall-1	4.0	sp3	All	All
Application	Checkpoint	Firewall-1	4.0	sp4	All	All
Application	Checkpoint	Firewall-1	4.0	sp5	All	All
Application	Checkpoint	Firewall-1	4.0	sp6	All	All

Application	Checkpoint	Firewall-1	4.0	sp7	All	All
Application	Checkpoint	Firewall-1	4.0	sp8	All	All
Application	Checkpoint	Firewall-1	4.1	All	All	All
Application	Checkpoint	Firewall-1	4.1	sp1	All	All
Application	Checkpoint	Firewall-1	4.1	sp2	All	All
Application	Checkpoint	Firewall-1	4.1	sp3	All	All
Application	Checkpoint	Firewall-1	4.1	sp4	All	All
Application	Checkpoint	Firewall-1	4.1	sp5	All	All
Application	Checkpoint	Firewall-1	4.0	All	All	All
Application	Checkpoint	Firewall-1	4.0	sp1	All	All
Application	Checkpoint	Firewall-1	4.0	sp2	All	All
Application	Checkpoint	Firewall-1	4.0	sp3	All	All
Application	Checkpoint	Firewall-1	4.0	sp4	All	All
Application	Checkpoint	Firewall-1	4.0	sp5	All	All
Application	Checkpoint	Firewall-1	4.0	sp6	All	All
Application	Checkpoint	Firewall-1	4.0	sp7	All	All
Application	Checkpoint	Firewall-1	4.0	sp8	All	All
Application	Checkpoint	Firewall-1	4.1	All	All	All
Application	Checkpoint	Firewall-1	4.1	sp1	All	All
Application	Checkpoint	Firewall-1	4.1	sp2	All	All
Application	Checkpoint	Firewall-1	4.1	sp3	All	All
Application	Checkpoint	Firewall-1	4.1	sp4	All	All
Application	Checkpoint	Firewall-1	4.1	sp5	All	All
Application	Checkpoint	Next Generation	All	All	All	All
Application	Checkpoint	Next Generation	All	All	All	All

References

Reference

20020308 Checkpoint FW1 SecuRemote/SecureClient "re-authentication" (client side hacks of users.C)
Check Point FW-1 SecuClient/SecuRemote Client Design Vulnerability
ISS X-Force Database: fw1-authentication-bypass-timeouts (8423): FireWall-1 SecuRemote/SecuClient authentication allows remote users to
CVE Program record
NVD vulnerability detail

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](#)