

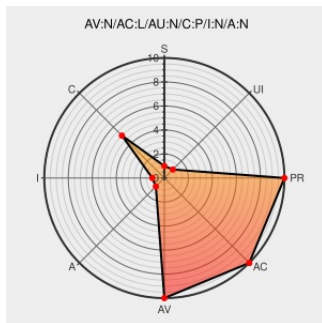


CVE-2002-1623

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1623

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Vpn-1 Firewall-1](#) from [Checkpoint](#) contain the following vulnerability:

The design of the Internet Key Exchange (IKE) protocol, when using Aggressive Mode for shared secret authentication, does not encrypt initiator or responder identities during negotiation, which may allow remote attackers to determine valid usernames by (1) monitoring responses before the password is supplied or (2) sniffing, as originally reported for FireWall-1 SecuRemote.

CVE-2002-1623 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

NTA in the news

www.nta-monitor.com
text/html

[MISC www.nta-monitor.com/news/checkpoint.htm](http://www.nta-monitor.com/news/checkpoint.htm)

'RE: SecuRemote usernames can be guessed or sniffed using IKE' - MARC

marc.info
text/html

[BUGTRAQ 20020911](http://bugtraq.20020911) RE: SecuRemote usernames can be guessed or sniffed using IKE

Sorry, the content you are trying to view does not exist. If you feel this message is in error, please email the webmaster.

[cve.report \(archive\)](http://cve.report)
text/html

[BID 5607](http://bid.5607)

Check Point Software Technologies: Alerts - IKE Aggressive Mode

web.archive.org
text/html
Inactive Link **Not Archived**

[CONFIRM](http://www.checkpoint.com/techsupport/alerts/ike.html)
www.checkpoint.com/techsupport/alerts/ike.html

[Full-Disclosure] Mailing List Charter	lists.grok.org.uk text/html Inactive Link Not Archived	 FULLDISC 20020903 Check Point statement on use of IKE Aggressive Mode
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF fw1-ike-username-enumeration(10034)
'Checkpoint FW-1 VPN Security Flaw (updated)' - SecuriTeam	Exploit www.securiteam.com text/html	 MISC www.securiteam.com/securitynews/5TP040U8AW.html
SecurityFocus HOME Mailing List: BugTraq	Exploit www.securityfocus.com text/html	 BUGTRAQ 20020903 SecuRemote usernames can be guessed or sniffed using IKE exchange
'RE: SecuRemote usernames can be guessed or sniffed using IKE exchange' - MARC	marc.info text/html	 BUGTRAQ 20020905 RE: SecuRemote usernames can be guessed or sniffed using IKE exchange
CERT/CC Vulnerability Note VU#886601	US Government Resource www.kb.cert.org text/html	 CERT-VN VU#886601

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkpoint	Vpn-1 Firewall-1	4.0	All	All	All
Application	Checkpoint	Vpn-1 Firewall-1	4.1	All	All	All
Application	Checkpoint	Vpn-1 Firewall-1	4.0	All	All	All
Application	Checkpoint	Vpn-1 Firewall-1	4.1	All	All	All
cpe:2.3:a:checkpoint:vpn-1_firewall-1:4.0:*:*:*:*.*						
cpe:2.3:a:checkpoint:vpn-1_firewall-1:4.1:*:*:*:*.*						
cpe:2.3:a:checkpoint:vpn-1_firewall-1:4.0:*:*:*:*.*						
cpe:2.3:a:checkpoint:vpn-1_firewall-1:4.1:*:*:*:*.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#).

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