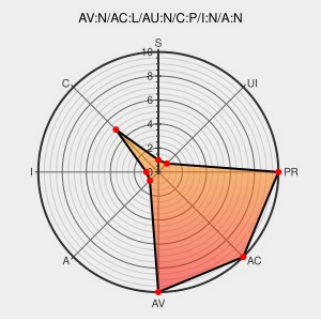
CVE-2002-1623

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 cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
NTA in the news	www.nta-monitor.com text/html	MISC www.nta-monitor.com/news/checkpoint.htm
'RE: SecuRemote usernames can be guessed or sniffed using IKE' - MARC	marc.info text/html	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) text/html	BID 5607
Check Point Software Technologies: Alerts - IKE Aggressive Mode	web.archive.org text/html Inactive Link Not Archived	CONFIRM 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

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→

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