



# CVE-2004-0040

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2004-0040
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-03-03 05:00:00 UTC
<b>Updated</b>	2017-10-10 01:30:00 UTC
<b>Description</b>	Stack-based buffer overflow in Check Point VPN-1 Server 4.1 through 4.1 SP6 and Check Point SecuRemote/SecureClient

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp1	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp2	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp3	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp4	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp5	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp5a	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	next_generation_fp0	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	next_generation_fp1	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	All	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp1	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp2	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp3	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp4	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp5	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	4.1	sp5a	All	All
Application	<a href="#">Checkpoint</a>	<a href="#">Firewall-1</a>	next_generation_fp0	All	All	All

Application	Checkpoint	Firewall-1	next_generation_fp1	All	All	All
Application	Checkpoint	Vpn-1	4.1	sp5a	All	All
Application	Checkpoint	Vpn-1	next_generation_fp0	All	All	All
Application	Checkpoint	Vpn-1	next_generation_fp1	All	All	All
Application	Checkpoint	Vpn-1	4.1	sp5a	All	All
Application	Checkpoint	Vpn-1	next_generation_fp0	All	All	All
Application	Checkpoint	Vpn-1	next_generation_fp1	All	All	All

## References

Reference	Source	Link
4432	OSVDB	<a href="http://www.osvdb.org">www.osvdb.org</a>
US-CERT Vulnerability Note VU#873334	CERT-VN	<a href="http://www.kb.cert.org">www.kb.cert.org</a>
O-073: Check Point VPN-1 Server and VPN Client Buffer Overflow Vulnerability	CIAC	<a href="http://www.ciac.org">www.ciac.org</a>
20040204 Checkpoint VPN-1/SecureClient ISAKMP Buffer Overflow	ISS	<a href="http://xforce.iss.net">xforce.iss.net</a>
3821	OSVDB	<a href="http://www.osvdb.org">www.osvdb.org</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.it">exchange.xforce.it</a>
20040205 Two checkpoint fw-1/vpn-1 vulns	BUGTRAQ	<a href="http://marc.info">marc.info</a>
Check Point VPN-1/SecuRemote ISAKMP Large Certificate Request Payload Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus">www.securityfocus</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org). This site includes MITRE data granted under the following [license](http://www.mitre.org).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)