



# CVE-2005-3768

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

## Summary

<b>CVE</b>	CVE-2005-3768
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-11-23 00:03:00 UTC
<b>Updated</b>	2011-03-08 02:27:00 UTC
<b>Description</b>	Buffer overflow in the Internet Key Exchange version 1 (IKEv1) implementation in Symantec Dynamic VPN Services, as use

## 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="#">Symantec</a>	<a href="#">Enterprise Firewall</a>	8.0	All	solaris	All
Application	<a href="#">Symantec</a>	<a href="#">Enterprise Firewall</a>	8.0	All	windows	All
Application	<a href="#">Symantec</a>	<a href="#">Enterprise Firewall</a>	8.0	All	solaris	All
Application	<a href="#">Symantec</a>	<a href="#">Enterprise Firewall</a>	8.0	All	windows	All
Hardware	<a href="#">Symantec</a>	<a href="#">Firewall Vpn Appliance 100</a>	All	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Firewall Vpn Appliance 100</a>	All	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Firewall Vpn Appliance 200</a>	All	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Firewall Vpn Appliance 200</a>	All	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 300</a>	2.0	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 300</a>	2.0	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 400</a>	2.0	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 400</a>	2.0	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 5000 Series</a>	3.0	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 5000 Series</a>	3.0	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 5100</a>	All	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 5100</a>	All	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 5300</a>	1.0	All	All	All

Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 5300</a>	1.0	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 5310</a>	1.0	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 5310</a>	1.0	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 5400</a>	2.0.1	All	All	All
Hardware	<a href="#">Symantec</a>	<a href="#">Gateway Security 5400</a>	2.0.1	All	All	All

## References

Reference	Source	Link
SecurityTracker.com Archives - Symantec Enterprise Firewall IPSec IKE Processing Lets Remote Users Deny Service	SECTRACK	<a href="#">s</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">v</a>
SecurityTracker.com Archives - Symantec Firewall/VPN Appliance IPSec IKE Processing Lets Remote Users Deny Service	SECTRACK	<a href="#">s</a>
Symantec Dynamic VPN Services: ISAKMP Denial of Service	CONFIRM	<a href="#">s</a>
SecurityTracker.com Archives - Symantec Gateway Security IPSec IKE Processing Lets Remote Users Deny Service	SECTRACK	<a href="#">s</a>
Secunia - Advisories - Symantec Firewall/VPN/Gateway ISAKMP Message Processing Denial of Service	SECUNIA	<a href="#">s</a>
CVE Program record	CVE.ORG	<a href="#">v</a>
NVD vulnerability detail	NVD	<a href="#">r</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](#) 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](#)