



CVE-2007-2174

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

Summary

CVE	CVE-2007-2174
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-24 16:19:00 UTC
Updated	2018-10-16 16:42:00 UTC
Description	The IOCTL handling in srescan.sys in the ZoneAlarm Spyware Removal Engine (SRE) in Check Point ZoneAlarm before 5.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkpoint	Zonealarm	All	All	All	All

References

Reference	Source
Check Point Zone Alarm Srescan.SYS Multiple Local Privilege Escalation Vulnerabilities	BID
ZoneAlarm 'srescan.sys' Driver Lets Local Users Gain System Privileges - SecurityTracker	SECTRACK
ZoneAlarm Products SRESCAN.SYS IOCTL Handler Privilege Escalation - Advisories - Secunia	SECUNIA
SecurityFocus	BUGTRAQ
Sun Cluster Remote USCSICMD IOCTL Processing Bug Lets Remote Authenticated Users Deny Service - SecurityTracker	SECTRACK
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
20070420 Check Point Zone Labs SRESCAN IOCTL Local Privilege Escalation Vulnerability	IDEFENSE
IBM X-Force Exchange	XF
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)