



CVE-2008-0350

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

Summary

CVE	CVE-2008-0350
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-18 00:00:00 UTC
Updated	2017-09-29 01:30:00 UTC
Description	admin/index.php in Evilsentinel 1.0.9 and earlier sends a redirect to the web browser but does not exit, which allows remote

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Evilsentinel	Evilsentinel	All	All	All	All

References

Reference	Source	Link
evilsentinel.altervista.org/forum/index.php	CONFIRM	evilsentinel.altervista.org/forum/index.php
Evilsentinel Administrator Login Security Bypass - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Evilsentinel 1.0.9 - Multiple Vulnerabilities Disable - PHP webapps Exploit	EXPLOIT-DB	www.exploit-db.com/exploits/10000/
Evilsentinel 1.0.9 Multiple Remote Vulnerabilities	BID	www.securityfocus.com/bid/32000
CVE Program record	CVE.ORG	www.cve.org/CVE/nvd/cve-2008-0350
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2008-0350

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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