



CVE-2011-1913

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

Summary

CVE	CVE-2011-1913
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-09-22 10:55:00 UTC
Updated	2017-08-17 01:34:00 UTC
Description	SQL injection vulnerability in the login form in the web interface in Mercator SENTINEL 2.0 allows remote attackers to execute arbitrary SQL commands via the 'username' parameter in the 'login' endpoint.

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mercator	Sentinel	2.0	All	All	All
Application	Mercator	Sentinel	2.0	All	All	All

References

Reference

IBM X-Force Exchange
Mercator Sentinel CVE-2011-1913 SQL Injection Vulnerability
Security Advisory SA46014 - Mercator Sentinel SQL Injection Vulnerability - Secunia
US-CERT Vulnerability Note VU#122142 - Mercator SENTINEL SQL injection allows authentication bypass
CERT-NPS:2011:005 Vulnérabilité Potentielle dans la solution de gestion de la sécurité opérationnelle des compagnies aériennes « Sentinel,
CERT-NPS:2011:005 – Escalade vers US-CERT.gov « CERT-NETPEAS
CVE Program record
NVD vulnerability detail

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)