



CVE-2008-0366

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

Summary

CVE	CVE-2008-0366
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-18 23:00:00 UTC
Updated	2018-10-15 21:59:00 UTC
Description	CORE FORCE before 0.95.172 does not properly validate arguments to SSDT hook handler functions in the Registry modu

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Core Security Technologies	Core Force	All	All	All	All

References

Reference	Source
SecurityFocus	BUGT
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPE
CORE FORCE Kernel Buffer Overflow - CXSecurity.com	SREA
Core Security Cyber Threat Prevention & Identity Governance	CONF
CORE FORCE - CORE FORCE R0.95 updated to address security vulnerabilities	CONF
CORE FORCE Firewall and Registry Modules Multiple Local Kernel Buffer Overflow Vulnerabilities	BID
SecurityTracker.com Archives - CORE FORCE Buffer Overflows and Input Validation Flaws Let Local Users Gain Elevated Privileges	SECT
CVE Program record	CVE.C
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](#).

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

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