



CVE-2006-2769

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2006-2769
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-02 10:18:00 UTC
Updated	2018-10-18 16:41:00 UTC
Description	The HTTP Inspect preprocessor (http_inspect) in Snort 2.4.0 through 2.4.4 allows remote attackers to bypass "uricontent" r

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sourcefire	Snort	2.4	All	All	All
Application	Sourcefire	Snort	2.4.1	All	All	All
Application	Sourcefire	Snort	2.4.2	All	All	All
Application	Sourcefire	Snort	2.4.3	All	All	All
Application	Sourcefire	Snort	2.4.4	All	All	All
Application	Sourcefire	Snort	2.4	All	All	All
Application	Sourcefire	Snort	2.4.1	All	All	All
Application	Sourcefire	Snort	2.4.2	All	All	All
Application	Sourcefire	Snort	2.4.3	All	All	All
Application	Sourcefire	Snort	2.4.4	All	All	All

References

Reference	Source	Link
'[Snort-devel] Snort Uricontent Bypass Vulnerability' - MARC	MLIST	marc.info
SecurityFocus	BUGTRAQ	www.securit
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.
SecurityFocus	BUGTRAQ	www.securit

Just a moment...	CONFIRM	www.snort.c
SUSE Updates for Multiple Packages - Advisories - Secunia	SECUNIA	secunia.com
SuSE Security announcements: [suse-security-announce] SUSE Security Summary Report SUSE-SR:2006:014	SUSE	lists.suse.cc
SecurityFocus	BUGTRAQ	www.securit
IBM X-Force Exchange	XF	exchange.xf
25837	OSVDB	www.osvdb
Snort URIContent Rules Detection Evasion Vulnerability	BID	www.securit
SecurityFocus	BUGTRAQ	www.securit
SecurityTracker.com Archives - Snort Lets Remote Users Bypass 'uricontent' Rules	SECTRACK	securitytrack
Demarc - Snort Bypass Vulnerability	MISC	www.demar
Snort HTTP Inspect Pre-Processor Uricontent Bypass - CXSecurity.com	SREASON	securityreas
Snort "http_inspect" Preprocessor Bypass Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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