



CVE-2015-2838

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

Summary

CVE	CVE-2015-2838
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-03 14:59:00 UTC
Updated	2018-10-09 19:56:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability in Nitro API in Citrix NetScaler before 10.5 build 52.3nc allows remote attack

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Netscaler	10.5	All	All	All
Application	Citrix	Netscaler	10.5	All	All	All

References

Reference	Source	Link	Tags
Citrix NITRO SDK - Command Injection Vulnerability	EXPLOIT-DB	www.exploit-db.com	
Full Disclosure: Command injection vulnerability in Citrix NITRO SDK xen_hotfix page	FULLDISC	seclists.org	
Securify	MISC	www.securify.nl	Exploit
SecurityFocus	BUGTRAQ	www.securityfocus.com	
Citrix NITRO SDK Command Injection ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit
Citrix NetScaler 'xen_hotfix' Page Command Injection Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](#)