



# CVE-2015-2841

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-2841
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-04-03 14:59:00 UTC
<b>Updated</b>	2016-12-03 03:06:00 UTC
<b>Description</b>	Citrix NetScaler AppFirewall, as used in NetScaler 10.5, allows remote attackers to bypass intended firewall restrictions via

## Risk And Classification

**Problem Types:** CWE-284

## 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
Exploit « Exploits Database by Offensive Security	EXPLOIT-DB
Citrix NetScaler HTTP Header Processing Flaw Lets Remote Users Bypass the Firewall in Certain Cases - SecurityTracker	SECTrack
Full Disclosure: Citrix Netscaler NS10.5 WAF Bypass via HTTP Header Pollution	FULLDISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

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