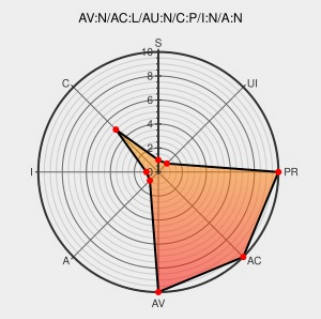
CVE-2015-4334

Published on: 12/07/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:06 PM UTC

CVE-2015-4334

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Proxysg Firmware from Symantec contain the following vulnerability:

The default configuration of SGOS in Blue Coat ProxySG before 6.2.16.5, 6.5 before 6.5.7.1, and 6.6 before 6.6.2.1 forwards authentication challenges from upstream origin content servers (OCS) when used in an explicit proxy deployment, which makes it easier for remote attackers to obtain sensitive information via a 407 (aka Proxy Authentication Required) HTTP status code, as demonstrated when using NTLM authentication.

CVE-2015-4334 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Blue Coat ProxySG Discloses NTLM Hashes to Remote Users - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1032149
Jonas Vestberg na Twitterze: "Updated security advisory from @BlueCoat https://t.co/TIS4O4UEt6 (and new title). They got a few things wrong:"	Third Party Advisory, nitter.domain.glass, text/html	MISC twitter.com/bugch3ck/status/591492380294979585
Broadcom Support Portal	Vendor Advisory, bto.bluecoat.com, text/html	CONFIRM bto.bluecoat.com/security-advisory/sa93

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Symantec	Proxysg Firmware	All	All	All	All
Operating System	Symantec	Proxysg Firmware	All	All	All	All
Operating System	Symantec	Proxysg Firmware	All	All	All	All

cpe:2.3:o:symantec:proxysg_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:symantec:proxysg_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:symantec:proxysg_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→