



CVE-2014-5348

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

Summary

CVE	CVE-2014-5348
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-19 19:55:00 UTC
Updated	2014-08-20 17:26:00 UTC
Description	Cross-site scripting (XSS) vulnerability in apps/zxtm/locallog.cgi in Riverbed Stingray (aka SteelApp) Traffic Manager Virtual Appliance

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Riverbed	Steelapp Traffic Manager	9.6	9620140312	All	All
Application	Riverbed	Steelapp Traffic Manager	9.6	9620140312	All	All

References

Reference	Source	Link
Full Disclosure: XSS Reflected vulnerability in RiverBed Stingray Traffic Manager Virtual Appliance V 9.6	FULLDISC	seclists.org
RiverBed Stingray Traffic Manager Virtual Appliance Cross Site Scripting Vulnerability	BID	www.securityfocus.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.

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](#)