



CVE-2015-3990

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

Summary

CVE	CVE-2015-3990
State	PUBLIC
Assigner	zdi-disclosures@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-20 18:59:00 UTC
Updated	2023-11-07 02:25:00 UTC
Description	The GMS ViewPoint (GMSVP) web application in Dell Sonicwall GMS, Analyzer, and UMA EM5000 before 7.2 SP4 allows

Risk And Classification

Problem Types: CWE-19

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sonicwall	Analyzer	All	All	All	All
Application	Sonicwall	Global Management System	All	All	All	All
Hardware	Sonicwall	Uma Em5000	-	All	All	All
Hardware	Sonicwall	Uma Em5000	-	All	All	All
Operating System	Sonicwall	Uma Em5000 Firmware	All	All	All	All

References

Reference

- SonicWALL Analyzer Product Notification
- Dell SonicWALL GMS/Analyzer Bugs Let Remote Users Obtain Potentially Sensitive Information and Remote Authenticated Users Execute Ar
- Zero Day Initiative
- Multiple Dell SonicWALL Products CVE-2015-3990 Remote Code Execution Vulnerability
- CVE Program record
- NVD vulnerability detail

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](#)