



# CVE-2015-0516

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

## Summary

<b>CVE</b>	CVE-2015-0516
<b>State</b>	PUBLIC
<b>Assigner</b>	security_alert@emc.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-01-21 15:17:00 UTC
<b>Updated</b>	2018-10-09 19:55:00 UTC
<b>Description</b>	Directory traversal vulnerability in EMC M&R (aka Watch4Net) before 6.5u1 and ViPR SRM before 3.6.1 allows remote authentication

## Risk And Classification

**Problem Types:** CWE-22

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Emc</a>	<a href="#">Vipr Srm</a>	All	All	All	All
Application	<a href="#">Emc</a>	<a href="#">Watch4net</a>	All	All	All	All

## References

### Reference

- EMC M&R/Watch4net Bugs Let Remote Users Obtain Passwords and Conduct Cross-Site Scripting Attacks and Let Remote Authenticated Users
- SecurityFocus
- Multiple EMC Products CVE-2015-0516 Directory Traversal Vulnerability
- Full Disclosure: Path traversal vulnerability in EMC M&R (Watch4net) MIB Browser
- Path traversal vulnerability in EMC M&R (Watch4net) MIB Browser - Security Advisories and Insights - Securify B.V.
- NEOHAPSIS - Peace of Mind Through Integrity and Insight
- 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](#).

**Free CVE JSON API** [cve.report/api](#)

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