



CVE-2013-0936

Published on: 03/28/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:39 PM UTC

CVE-2013-0936

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Smarts Ip Manager](#) from [Emc](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in EMC Smarts IP Manager, Smarts Service Assurance Manager, Smarts Server Manager, Smarts VoIP Availability Manager, Smarts Network Protocol Manager, and Smarts MPLS Manager before 9.2 allows remote attackers to inject arbitrary web script or HTML via a crafted URL.

CVE-2013-0936 has been assigned by [security_alert@emc.com](#) to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
No Description Provided	archives.neohapsis.com	BUGTRAQ 20130327 ESA-2013-018: EMC Smarts Product - Cross Site Scripting Vulnerability
	Inactive Link Not Archived	

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
Application	Emc	Smarts Ip Manager	9.1	All	All	All
Application	Emc	Smarts Ip Manager	9.1	All	All	All
Application	Emc	Smarts Mpls Manager	9.1	All	All	All
Application	Emc	Smarts Mpls Manager	9.1	All	All	All
Application	Emc	Smarts Network Protocol Manager	9.1	All	All	All
Application	Emc	Smarts Network Protocol Manager	9.1	All	All	All
Application	Emc	Smarts Server Manager	9.1	All	All	All
Application	Emc	Smarts Server Manager	9.1	All	All	All
Application	Emc	Smarts Services Assurance Manager	9.1	All	All	All
Application	Emc	Smarts Services Assurance Manager	9.1	All	All	All
Application	Emc	Smarts Voip Availability Manager	9.1	All	All	All
Application	Emc	Smarts Voip Availability Manager	9.1	All	All	All
cpe:2.3:a:emc:smarts_ip_manager:9.1:*****:						
cpe:2.3:a:emc:smarts_ip_manager:9.1:*****:						
cpe:2.3:a:emc:smarts_mpls_manager:9.1:*****:						
cpe:2.3:a:emc:smarts_mpls_manager:9.1:*****:						
cpe:2.3:a:emc:smarts_network_protocol_manager:9.1:*****:						
cpe:2.3:a:emc:smarts_network_protocol_manager:9.1:*****:						
cpe:2.3:a:emc:smarts_server_manager:9.1:*****:						
cpe:2.3:a:emc:smarts_server_manager:9.1:*****:						
cpe:2.3:a:emc:smarts_services_assurance_manager:9.1:*****:						
cpe:2.3:a:emc:smarts_services_assurance_manager:9.1:*****:						
cpe:2.3:a:emc:smarts_voip_availability_manager:9.1:*****:						
cpe:2.3:a:emc:smarts_voip_availability_manager:9.1:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

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](#)