



CVE-2012-2590

Published on: 08/12/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:26 PM UTC

CVE-2012-2590

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Escon Supportportal](#) from [E-supportportal](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in ESCON SupportPortal Professional Edition 3.0 allow remote attackers to inject arbitrary web script or HTML via an e-mail message body with (1) a SCRIPT element, (2) a crafted SRC attribute of an IFRAME element, (3) a crafted CONTENT attribute of an HTTP-EQUIV="Set-Cookie" META element, or (4) an innerHTML attribute within an XML document.

CVE-2012-2590 has been assigned by cert@cert.org 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
ESCON SupportPortal Pro 3.0 Stored XSS	Exploit www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 20350

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	E-supportportal	Escon Supportportal	3.0	All	professional	All
Application	E-supportportal	Escon Supportportal	3.0	All	professional	All
cpe:2.3:a:e-supportportal:escon_supportportal:3.0:*:professional:*****:						
cpe:2.3:a:e-supportportal:escon_supportportal:3.0:*:professional:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		