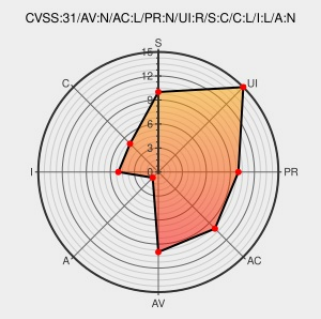
CVE-2013-6880

Published on: 11/22/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:38 PM UTC

CVE-2013-6880

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Flashcanvas from Elvedia contain the following vulnerability:

Open redirect in proxy.php in FlashCanvas before 1.6 allows remote attackers to redirect users to arbitrary web sites and conduct cross-site scripting (XSS) attacks via the HTTP Referer header.

CVE-2013-6880 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

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
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	MISC exchange.xforce.ibmcloud.com/vulnerabilities/89663

CVE-2013-6880 Proof of Concept - 7 Elements	Exploit Third Party Advisory www.7elements.co.uk text/html	MISC www.7elements.co.uk/resources/blog/cve-2013-6880-proof-concept
No Description Provided	Broken Link archives.neohapsis.com Inactive Link Not Archived	MISC archives.neohapsis.com/archives/bugtraq/2013-12/0051.html
CVE-2013-6880 FlashCanvas proxy.php XSS Vulnerability - 7 Elements	Third Party Advisory www.7elements.co.uk text/html	MISC www.7elements.co.uk/news/cve-2013-6880

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	Elvedia	Flashcanvas	All	All	All	All
Application	Elvedia	Flashcanvas	All	All	All	All

cpe:2.3:a:elvedia:flashcanvas:*:*:*:*:*:*:*:*:

cpe:2.3:a:elvedia:flashcanvas:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→