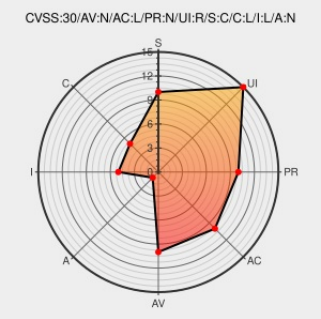
CVE-2017-15646

Published on: 10/19/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:33 PM UTC

CVE-2017-15646

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



Certain versions of Webmin from Webmin contain the following vulnerability:

Webmin before 1.860 has XSS with resultant remote code execution. Under the 'Others/File Manager' menu, there is a 'Download from remote URL' option to download a file from a remote server. After setting up a malicious server, one can wait for a file download request and then send an XSS payload that will lead to Remote Code Execution, as demonstrated by an OS command in the value attribute of a name='cmd' input element.

CVE-2017-15646 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
Webmin	Vendor Advisory	MISC:www.webmin.com/security.html

Webmin	Vendor Advisory www.webmin.com text/html	MISC www.webmin.com/security.html
Webmin	Release Notes Vendor Advisory www.webmin.com text/html	MISC www.webmin.com/changes.html
401 Authorization Required	Exploit Third Party Advisory blogs.securiteam.com text/html Inactive Link Not Archived	MISC blogs.securiteam.com/index.php/archives/3430
Escape potentially malicious HTTP headers · webmin/webmin@0c58892 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/webmin/webmin/commit/0c58892732ee7610a7abba5507614366d382c9

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	Webmin	Webmin	All	All	All	All

cpe:2.3:a:webmin:webmin:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→