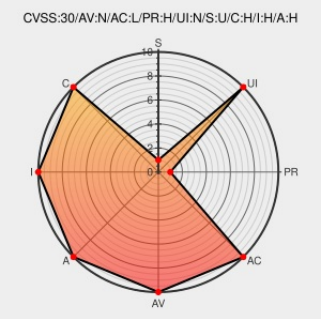
CVE-2015-1445

Published on: 08/28/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:09 PM UTC

CVE-2015-1445

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



Certain versions of Fli4l from Fli4l contain the following vulnerability:

HTTP header injection in the httpd package in fli4l before 3.10.1 and 4.0 before 2015-01-30.

CVE-2015-1445 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
oss-security - Re: RCE, XSS and HTTP header injection in fli4l web interface	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20150201 Re: RCE, XSS and HTTP header injection in fli4l web interface

oss-sec: RCE, XSS and HTTP header injection in fli4l web interface	Mailing List Third Party Advisory seclists.org text/html	MLIST [oss-security] 20150131 RCE, XSS and HTTP header injection in fli4l web interface
	Mitigation Vendor Advisory www.fli4l.de text/plain	CONFIRM www.fli4l.de/fileadmin/fli4l/security/advisory-FFL-1113.txt

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fli4l	Fli4l	4.0	All	All	All
Operating System	Fli4l	Fli4l	4.0	All	All	All
Operating System	Fli4l	Fli4l	All	All	All	All

cpe:2.3:o:fli4l:fli4l:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:fli4l:fli4l:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:fli4l:fli4l:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→