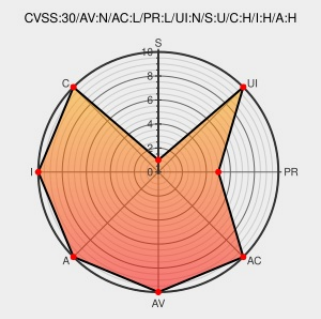
CVE-2018-19114

Published on: 11/08/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:40 PM UTC

CVE-2018-19114

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



Certain versions of Mindoc from Iminho contain the following vulnerability:

An issue was discovered in MinDoc through v1.0.2. It allows attackers to gain privileges by uploading an image file with contents that represent an admin session, and then sending a Cookie: header with a mindoc_id value containing the relative pathname of this uploaded file. For example, the mindoc_id (aka session ID) could be of the form aa/../../uploads/blog/201811/attach_#.jpg where '#' is a hex value displayed in the upload field of a manage/blogs/edit/ screen.

CVE-2018-19114 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
allow attacker unauthorized access to user account · Issue #384		MISC

allow attacker unauthorized access to user account · Issue #384 · lifei6671/mindoc · GitHub

Issue Tracking
Third Party Advisory
github.com
text/html

MISC
github.com/lifei6671/mindoc/issues/384

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Iminho	Mindoc	All	All	All	All

cpe:2.3:a:iminho:mindoc:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→