alacerda / **mkauth_19.01_user_impersonation**

Created 2 years ago

☆ Star

<> Code -o- Revisions 1

Mk-Auth User Impersonation Via Reflected XSS and Unprotected Session Cookie

mkauth_19.01_user_impersonation

```
Mk-Auth User Impersonation Via Reflected XSS and Unprotected Session Cookie

Product Description:
Mk-Auth is a Brazilian Management System for Internet Service Providers used to control client access and permissions via a web interface p
Vulnerability Description:
It is possible to steal and reuse an admin session token by abusing a reflected XSS and an unprotected cookie.
Additional Information:
The session token (centralmka2) does not have the HTTPOnly flag set what allows a javascript code to read its content. In addition to that,
http://<mkserver>/admin/logs_ajax.php?registro=0&tipo=todos%27%3balert(document.cookie)%2f%2f
Vulnerability Type:
CWE-79: Improper Neutralization of Input During Web Page Generation
CWE-1004: Sensitive Cookie Without ‘HTTPOnly’ Flag
Vendor:
Mk-Auth
Affected Product:
MK-Auth 19.01 :: K4.9
Probably previous are also affected
Affected Component:
Admin: Logs
Attack Vector:
Remote
Code Execution:
No
Attack Vector:
A logged administrator or support user must click on a malicious link.
Reference:
        http://mk-auth.com.br/
Discoverer:
Alan Lacerda (alacerda) | alacerda[at]intruderlabs.com.br
Filipe Cordeiro (sknux) | c_sfilipe[at]outlook.com
```