Mk-Auth Remote Command Execution (RCE) via File Upload

Product Description:

Mk-Auth is a Brazilian Management System for Internet Service Providers used to control client access and permissions via a web interface panel.

Vulnerability Description:

It is possible to bypass the upload protection on the User Profile feature to upload any arbitrary file. This vulnerability may be used to perform a Remote Command Execution

Additional Information:

The upload form only accepts files with the .png extension but it is possible to bypass its security mechanism by adding a double extension to the filename. Ex.: malicious_file.png.php

Vulnerability Type:

CWE-434: Unrestricted Upload of File with Dangerous Type

Vendor:

Mk-Auth

Affected Product:

MK-Auth 19.01 :: K4.9

Probably previous are also affected

Affected Component:

User Profile: Photo Upload

Attack Vector:

Remote

Code Execution:

Yes

Attack Vector:

Any client of the Internet Service Provider that has access to the platform (to download billings and request for support) may exploit this vulnerability.

Reference:

http://mk-auth.com.br/

Discoverer:

alacerda (velocista)| Kitsun3Sec | alacerda[at]intruderlabs.com.br