THE ASHGABAT TIMES

# Hackers have attacked the Samsung MagicINFO platform.

A critical vulnerability in the Samsung MagicINFO 9 Server platform, discovered in August 2024, has begun to be actively exploited by hackers following the publication of the exploit code, researchers from Arctic Wolf reported.

The vulnerability, identified as CVE-2024−7399, allows attackers to upload malicious files to the server without authorization, gaining full control over the system. This is particularly dangerous as MagicINFO manages screens in stores, airports, and offices.

The issue stems from insufficient file upload verification: the server does not filter file names and extensions, allowing hackers to place malicious JSP files (JavaServer Pages) and execute arbitrary commands. As a result, devices may become part of the Mirai botnet, used for cyberattacks. The exploit has already been observed in attacks.

Samsung has patched the vulnerability in version 21.1050, and the company strongly recommends updating the servers. Arctic Wolf advises organizations to limit internet access to servers and enhance monitoring. The vulnerability has a CVSS rating of 8.8.