Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Samsung Patches Actively Exploited MagicINFO 9 Server Zero-Day

Date of Publication	Admiralty Code	TA Number
May 15, 2025	A1	TA2025149

Summary

First Seen: April 2025
Affected Products: Samsung MagicInfo 9 Server
Malware: Mirai
Impact: A critical vulnerability (CVE-2025-4632) in Samsung's MagicINFO 9 Server is being actively exploited by attackers to gain system-level access and deploy malicious payloads. This path traversal flaw allows attackers to write arbitrary files with system-level privileges. Signs of compromise have been observed in real-world environments, including attempts to deploy Mirai malware. Organizations using MagicINFO are strongly urged to act quickly and apply patches immediately.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-4632	Samsung MagicINFO 9 Server Path Traversal Vulnerability	Samsung MagicInfo 9 Server	✓	✗	✓
CVE-2024-7399	Samsung MagicINFO 9 Server Path Traversal Vulnerability	Samsung MagicInfo 9 Server	✗	✗	✓

Vulnerability Details

#1

Samsung has addressed a critical zero-day vulnerability in its MagicINFO 9 Server platform, which is already being actively exploited in the wild. Tracked as CVE-2025-4632, the flaw is a path traversal vulnerability that allows attackers to write arbitrary files to the system with elevated privileges potentially granting them full control over the server.

#2 This vulnerability bears a striking resemblance to CVE-2024-7399, a critical flaw disclosed in August 2024 that Samsung claimed was patched in version 21.1050. Consequently, attackers have continued targeting MagicINFO 9 Server instances, including those running what was believed to be the latest version.

#3 The issue came to light after cybersecurity researchers detected suspicious activity on fully updated servers. Their investigation revealed CVE-2025-4632 and uncovered three incidents in which threat actors used the flaw to download malicious payloads such as srvany.exe and services.exe, and execute reconnaissance commands, likely in attempts to establish persistence or move laterally within the environment.

#4 In several cases, the vulnerability was exploited to deploy the Mirai botnet, demonstrating that real-world exploitation is already underway. CVE-2025-4632 effectively serves as a patch bypass for CVE-2024-7399, underscoring the need for rigorous patch validation and ongoing security assessments. If your organization uses MagicINFO 9 Server, it’s crucial to install the latest updates without delay. This will help close the security gap and protect your systems from ongoing attacks.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-4632	Samsung MagicInfo 9 Server Versions prior to 21.1052	cpe:2.3:a:samsung:magicinfo_9_server:*:*:*:*:*:*:*:*	CWE-22
CVE-2024-7399	Samsung MagicINFO 9 Server Versions prior to 21.1050	cpe:2.3:a:samsung:magicinfo_9_server:*:*:*:*:*:*:*:*	CWE-22 CWE-434

Recommendations

Update Immediately: Install Samsung’s latest security update to address CVE-2025-4632. This is the most effective way to prevent attackers from gaining system-level access. Make sure to update to version 21.1052 or later.

Limit Who Can Reach Your MagicINFO Server: If your MagicINFO server is exposed to the internet, it's a good idea to tighten access. Place it behind a VPN or firewall and allow only trusted IP addresses to connect. This helps keep attackers from easily finding and targeting your system.

Reduce File Write Access to Critical Directories Restrict the ability of the MagicINFO application and any connected users to write files to sensitive system areas. By limiting write permissions, you can significantly reduce the impact if an attacker attempts to exploit the vulnerability and gain system-level access.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation	

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp[:]//185[.]225[.]226[.]53/php_cli[.]exe, hxxp[:]//185[.]225[.]226[.]53/srvany[.]exe
File Path	C:\MagicInfo Premium\tomcat\bin\php-cli.exe, C:\MagicInfo Premium\tomcat\bin\php-fpm.exe
SHA256	c9c464c872b539eee7481e15331b7a6c75f4ba1f24b64d9f36a70b87a164d122, abd4afd71b3c2bd3f741bbe3cec52c4fa63ac78d353101d2e7dc4de2725d1ca1

Patch Details

Update your Samsung MagicInfo 9 Server to the latest version 21.1052 to address the flaw.

Link:
https://eu.community.samsung.com/t5/samsung-solutions/update-magicinfo-server-v9-21-1052-0-setup-file/ta-p/11374265

References

https://security.samsungtv.com/securityUpdates#SVP-MAY-2025

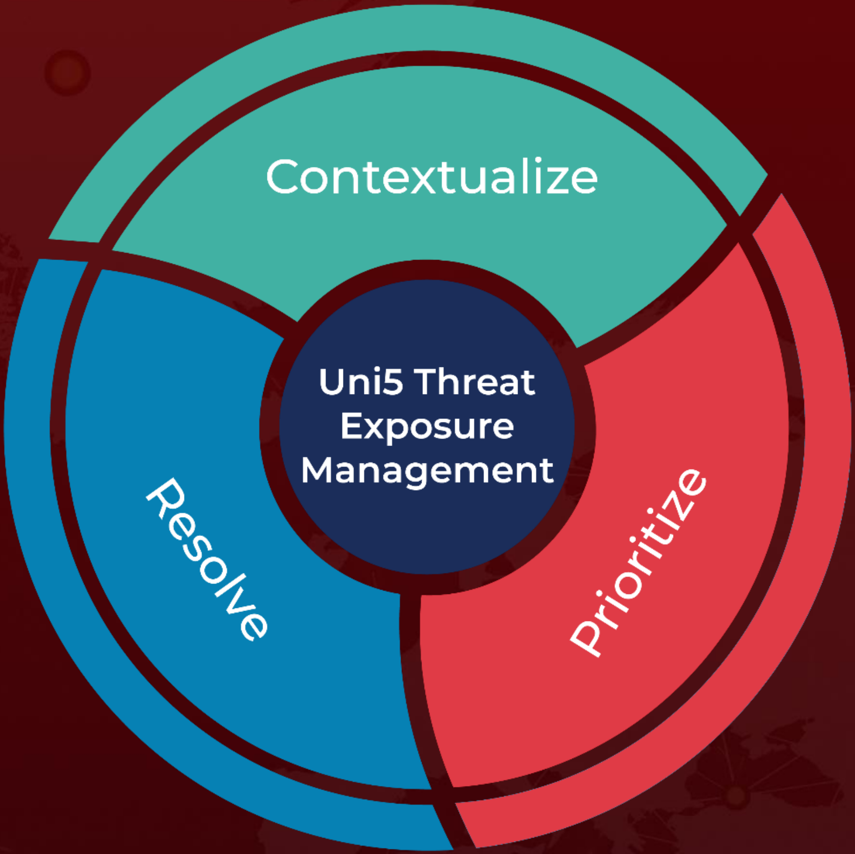
https://www.huntress.com/blog/post-exploitation-activities-observed-from-samsung-magicinfo-9-server-flaw

https://security.samsungtv.com/securityUpdates

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 15, 2025 • 4:00 AM

More at www.hivepro.com