CVE-2024-7399

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-7399
State	PUBLISHED
Assigner	samsung.tv_appliance
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-08-12 13:38:41 UTC
Updated	2026-04-24 20:23:57 UTC
Description	Improper limitation of a pathname to a restricted directory vulnerability in Samsung MagicINFO 9 Server version before 21.1

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.709960000 probability, percentile 0.987130000 (date 2026-04-24)

CISA KEV: Listed on 2026-04-24; due 2026-05-08; ransomware use Unknown

Problem Types: CWE-22 | CWE-434 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	PSIRT@samsung.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CISA Known Exploited Vulnerability

Vendor	Samsung
Product	MagicINFO 9 Server
Name	Samsung MagicINFO 9 Server Path Traversal Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://security.samsungtv.com/securityUpdates ; https://nvd.nist.gov/vuln/detail/CVE-2024-7399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samsung	Magicinfo 9 Server	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Samsung Electronics	MagicINFO 9 Server	affected 21.1050 custom	Windows

References

Reference	Source	Link
arcticwolf.com/resources/blog-uk/arctic-wolf-observes-exploitation-of-path-t...	134c704f-9b21-4f2e-91b3-4a467353bcc0	arcticwolf.com
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov
security.samsungtv.com/securityUpdates	PSIRT@samsung.com	security.samsungt
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

Vendor Comments And Credit

Discovery Credit

CNA: Anonymous working with Trend Mirco Zero Day Initiative (en)

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**