Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

JAVS Courtroom Recording Software Hit by Supply Chain Attack

Date of Publication	Admiralty Code	TA Number
May 28, 2024	A1	TA2024210

Summary

Attack Commenced: April 2024
Affected Product: JAVS Viewer software
Malware: RustDoor, GateDoor
Impact: Attackers have compromised the installer for Justice AV Solutions (JAVS), a popular courtroom video recording software, with sophisticated RustDoor and GateDoor malware. This critical supply chain attack, identified as CVE-2024-4978, enables the malware to transmit detailed system information to its command-and-control server, allowing attackers to seize control of affected systems.

⚙ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-4978	JAVS Arbitrary code Execution Vulnerability	JAVS Viewer software	✗	✗	✓

Vulnerability Details

#1 Adversaries have backdoored the installer for the widely used Justice AV Solutions (JAVS) courtroom video recording software with RustDoor and GateDoor malware, enabling them to take control of compromised systems. JAVS technologies, implemented in over 10,000 locations worldwide, are integral to courtrooms, chambers, jury rooms, jail and prison facilities, as well as council, hearing, and lecture rooms. This supply chain attack is tracked as CVE-2024-4978.

#2 The installer includes a loader linked to the GateDoor/Rustdoor malware family, which facilitates unauthorized remote access, collects data from the host computer, and downloads additional malicious payloads. RustDoor was initially identified in December 2023, with its Windows variant known as GateDoor, written in Golang instead of Rust. JAVS has removed the compromised JAVS Viewer version 8.3.7 from its official website.

#3 The trojanized software featured a malicious ffmpeg.exe binary signed with an unexpected Authenticode signature. Upon execution, the malware transmits system information to its command-and-control (C2) server via Windows sockets and WinHTTP requests. Once connected, it relays detailed data about the compromised host, including hostname, operating system details, processor architecture, program working directory, and username.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-4978	JAVS Viewer Software Version 8.3.7	cpe:2.3:a:justice_av_solutions:viewer:*:*:*:*:*:*:*	CWE-506

Recommendations

Reimaging Endpoints: It's crucial to reimage any endpoints where JAVS Viewer 8.3.7 was installed. Simply uninstalling the software won't suffice, as attackers might have implanted additional backdoors or malware. Reimaging ensures a fresh start. Completely reimagining affected endpoints and resetting associated credentials is vital to prevent attackers from persisting through backdoors or using stolen credentials.

Installing the Latest Version of JAVS Viewer: Upgrade the JAVS Viewer software to version 8.3.9 or higher, the latest safe version, after reimaging the systems. Users with version 8.3.7 of the JAVS Viewer executable installed are at high risk and should take immediate action.

Vendor and Third-Party Risk Management: Regularly assess the security posture of third-party vendors and service providers involved in the ecosystem. Ensure that vendors adhere to security best practices and compliance requirements to minimize supply chain risks.

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	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact	T1059 Command and Scripting Interpreter
T1587 Develop Capabilities	T1587.002 Code Signing Certificates	T1587.001 Malware	T1608 Stage Capabilities
T1195 Supply Chain Compromise	T1588.006 Vulnerabilities	T1059.001 PowerShell	T1059.006 Python
T1204.002 Malicious File	T1546.016 Installer Packages	T1036 Masquerading	T1027.009 Embedded Payloads
T1212 Exploitation for Credential Access	T1082 System Information Discovery	T1105 Ingress Tool Transfer	T1041 Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	JAVS.Viewer8.Setup_8.3.7.250-1.exe, fffmpeg.exe, Chrome_installer.exe, Main.exe, Dll2.dll, firefox_updater.exe, ChromeDiscovery.exe, OneDriveStandaloneUpdater.exe

TYPE	VALUE
URLs	hxxps[:]//www[.]javs[.]com/download/45819/, hxxps[:]//45[.]120[.]177[.]178/gateway/register, hxxps[:]//45[.]120[.]177[.]178/gateway/report
IPv4	45[.]120[.]177[.]178
SHA256	aace6f617ef7e2e877f3ba8fc8d82da9d9424507359bb7dcf6b81c889a755535, fe408e2df48237b11cb724fa51b6d5e9c74c8f5d5b2955c22962095c7ed70b2c, a5e24c10d595969858af422c6dff6bed5f9c6c49dc9622d694327323d8a57d72, f8a734d5e7a7b99b29182dddf804d5daa9d876bf39ce7a04721794367a73da51, 4150452d8041a6ec73c447cbe3b1422203fffdfbf5c845dbac1bed74b33a5e09, 2183c102c107d11ae8aa1e9c0f2af3dc8fa462d0683a033d62a982364a0100d0, 4f0ca76987edfe00022c8b9c48ad239229ea88532e2b7a7cd6811ae353cd1eda, d8def4437bd76279ec6351b65156d670ec0fed24d904e6648de536fed1061671, C65ee0f73f53b287654b6446ffe7264e0d93b24302e7f0036f5e7db3748749b9

Patch Details

Upgrade to the latest version of JAVS Viewer, version 8.3.8 or higher

Link:
https://www.javs.com/downloads/

References

https://www.rapid7.com/blog/post/2024/05/23/cve-2024-4978-backdoored-justice-av-solutions-viewer-software-used-in-apparent-supply-chain-attack/

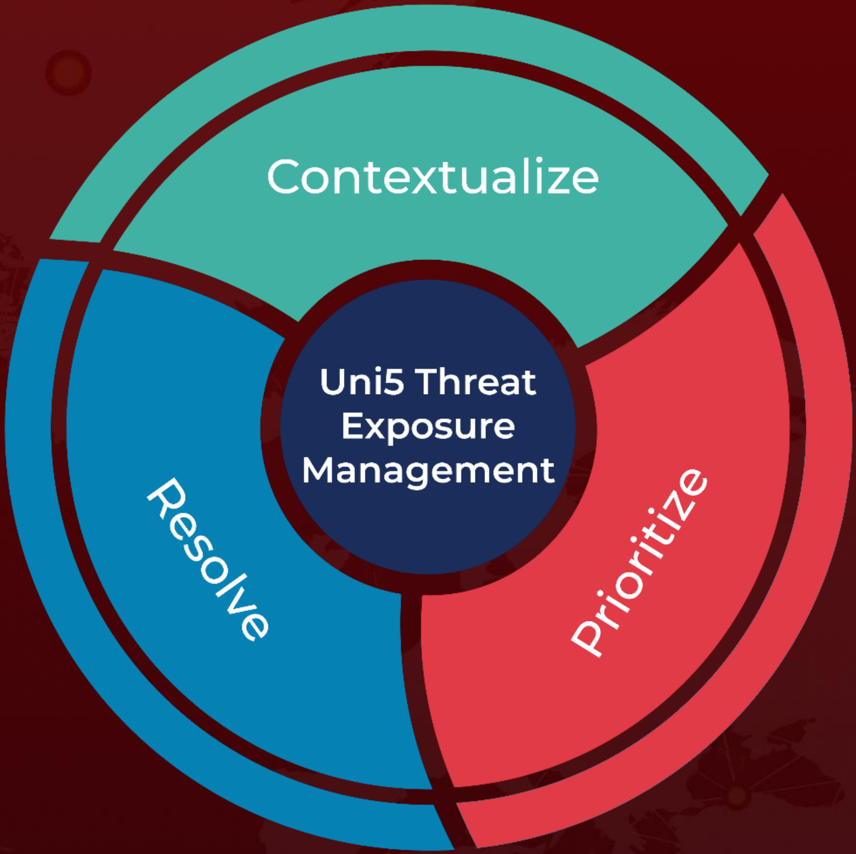
https://medium.com/s2wblog/rustdoor-and-gatedoor-a-new-pair-of-weapons-disguised-as-legitimate-software-by-suspected-34c94e558b40

https://www.hivepro.com/threat-advisory/smoothoperator-campaign-trojanizes-3cxdesktopapp/

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 28, 2024 • 10:30 PM

More at www.hivepro.com