مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Backdoored Justice AV Solutions Viewer Software

Tracking #:432315894

Date:27-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a backdoor is hidden within the Justice AV Solutions Viewer installer that allows attackers to remotely run unauthorized PowerShell commands on system.

TECHNICAL DETAILS:

Justice AV Solutions Viewer Setup 8.3.7.250-1 contains a malicious binary when executed and is signed with an unexpected authenticode signature. A remote, privileged threat actor may exploit this vulnerability to execute of unauthorized PowerShell commands. **CVE-2024-4978** is the CVE assigned.

- **Malicious Software:** A backdoor is hidden within the Justice AV Solutions Viewer installer (version 8.3.7.250-1). This backdoor is disguised with a valid digital certificate, making it appear legitimate.
- **Attack Method**: When the installer is executed, the backdoor allows attackers to remotely run unauthorized PowerShell commands on system. This could be used to steal data, install additional malware, or disrupt critical systems.
- **Impact**: Organization that uses Justice AV Solutions Viewer 8.3.7, systems are at high risk of being compromised.
- Threat Actors has now developed a Windows version that merges with Gate Door.

Related IOCs:

- SHA256(Dropper):
  fe408e2df48237b11cb724fa51b6d5e9c74c8f5d5b2955c22962095c7ed70b2c
- SHA256 (RustDoor):
  aace6f617ef7e2e877f3ba8fc8d82da9d9424507359bb7dcf6b81c889a755535
- SHA256 (chrome_installer.exe)
  f8a734d5e7a7b99b29182dddf804d5daa9d876bf39ce7a04721794367a73da51
- SHA256(firefox_updater.exe)
  4f0ca76987edfe00022c8b9c48ad239229ea88532e2b7a7cd6811ae353cd1eda

Remediation:

- Immediately reimage any endpoints where JAVS Viewer 8.3.7 was installed. Uninstalling the software is not enough, as the backdoor may have already infected systems.
- Reset Credentials: Reset passwords for all accounts that were used on affected systems, including local accounts and any remote accounts accessed during the time JAVS Viewer 8.3.7 was installed.
- Web Browsers: Reset credentials used in web browsers on affected endpoints, as attackers may have stolen cookies or other sensitive information.

- Update Software: After reimaging, install the latest version of JAVS Viewer (8.3.8 or higher). This version does not contain the backdoor.
- Avoid Untrusted Sources: Only download software from the official vendor or trusted sources.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the latest version of JAVS Viewer and apply remediation.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

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/