Cactus Ransomware Exploiting Qlik Sense Code Execution Vulnerability

Date: 15th December 2023 | Severity: High

Summary

A new Cactus Ransomware was exploited in the code execution vulnerability to Qlik Sense for initial access.

Cactus is ransomware that encrypts data, provides a ransom note (" cAcTuS.readme.txt "), and appends the. "CTS1" extension to filenames. They exploit via the combination or direct abuse of (CVE-2023-41266, CVE-2023-41265).

Attack Vectors

CVE-2023-41266 Path traversal in Qlik Sense Enterprise for Windows. The severity range is high (8.2). An unauthenticated, remote attacker generates an anonymous session, which allows them to perform HTTP requests to unauthorized endpoints.

CVE-2023-41265 HTTP Tunneling vulnerability in Qlik Sense Enterprise for Windows, severity range is critical (9.6). Allowing them to execute HTTP requests on the backend server hosting the repository application.

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	949d9523269604db26065f002feef9ae de6ce47e28337d28b6d29ff61980b2e9 5737cb3a9a6d22e957cf747986eeb1b3 2611833c12aa97d3b14d2ed541df06b2 1add9766eb649496bc2fa516902a5965 e28db6a65da2ebcf304873c9a5ed086d eba1596272ff695a1219b1380468293a 173f9b0db97097676a028b4b877630adc7281d2f cb570234349507a204c558fc8c4ecf713e2c0ac35c93052713f317431bf232a2894658a3a4ebfad9 884cebf1ad0e65f4da60c04bc31f62f796f90d79 be903ded39cbc8332cefd9ebbe7a66d95e9d6522 060a5d189ccf3fc32a758f1e218f814f6ce81744 3c887ece654ea46b1778d3c7a8a6a7c7c7cfa61c c806c7006950dea6c20d3d2800fe46d9350266b6
Domain	sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid.onion cactusbloguuodvqjmnzlwetjlpj6aggc6iocwhuupb47laukux7ckid.
IPs	No ips found.

Recommendation

Submit the File Hash to the Antivirus team to update their database with the file hashes. Block all IOCs at controls. Make regular backups of important and critical files.

Submit the File Hash to the Antivirus team to update their database with the file hashes.

Submit the IPs to Network team to block in the firewall.

Block the Domain in the Proxy.

Make regular backups of important and critical files.

Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.

Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

https://otx.alienvault.com/pulse/64ba02ecb2d2743614f9606a

https://gbhackers.com/cactus-ransomware-qlik/