

HiveForce Labs

# THREAT ADVISORY

**ATTACK REPORT**

## Cactus Ransomware Exploits Vulnerabilities in Qlik Sense

Date of Publication

December 1, 2023

Admiralty Code

A1

TA Number

TA2023484

# Summary

**Attack Began:** November 2023

**Malware:** Cactus ransomware

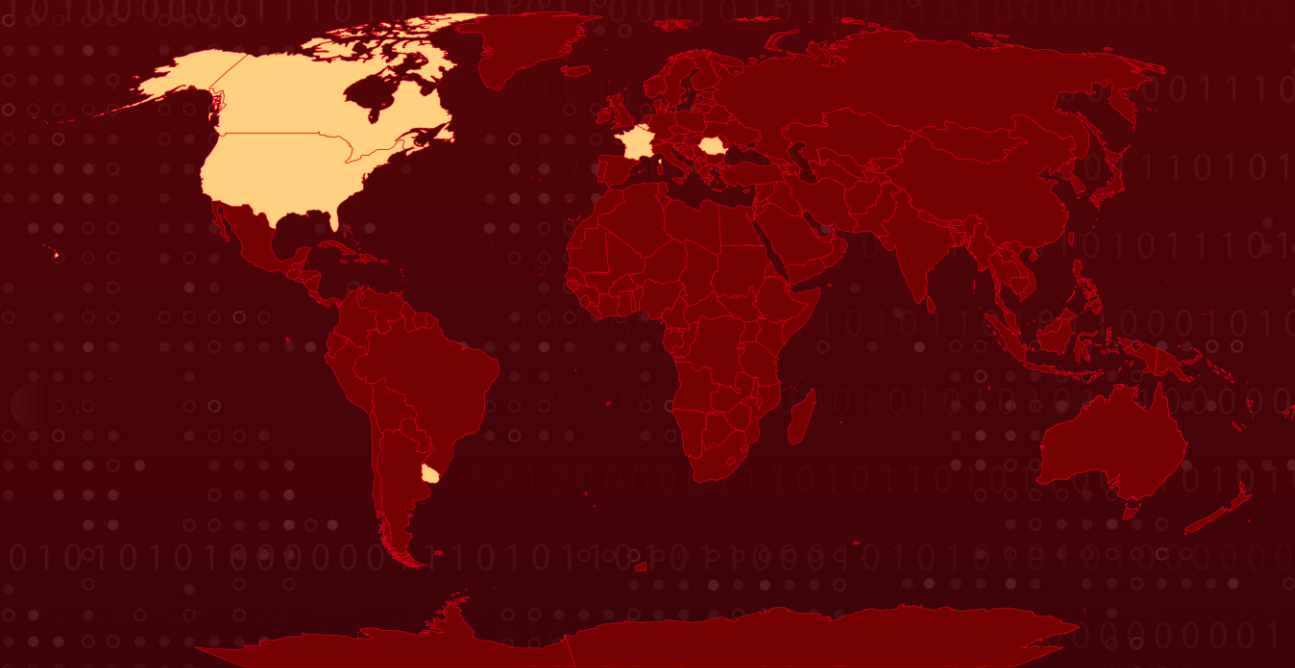
**Attack Region:** France, Canada, United States, Uruguay, Romania, Belgium

**Targeted Industries:** Hospitality, Healthcare, Technology, Construction, Engineering, Commercial Services

**Affected Products:** Qlik Sense Enterprise for Windows

**Attack:** The Cactus ransomware is actively exploiting critical Qlik Sense vulnerabilities, with the ultimate goal of establishing persistence and enabling remote control, infiltrating corporate networks stealthily. This serves as a stark reminder that unpatched Qlik Sense instances are prime targets for this relentless threat.







## 🗡️ Attack Regions



## ⚙️ CVEs

Powered by Bing  
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-41266	Qlik Sense Enterprise path traversal vulnerability	Qlik Sense Enterprise for Windows	❌	✅	✅

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-41265	Qlik Sense Enterprise Privilege escalation vulnerability	Qlik Sense Enterprise for Windows			
CVE-2023-48365	Qlik Sense Enterprise remote code execution vulnerability	Qlik Sense Enterprise for Windows			

# Attack Details

## #1

The **Cactus** ransomware has been capitalizing on critical vulnerabilities within the Qlik Sense data analytics solution to gain initial entry into corporate networks. The successful exploitation of these weaknesses is followed by the manipulation of the Qlik Sense Scheduler service, initiating processes aimed at downloading additional tools to establish persistence and enable remote control.

## #2

To achieve this, threat actors utilized PowerShell and the Background Intelligent Transfer Service (BITS) for downloading supplementary tools, ensuring the establishment of persistence and securing remote control. In late August, the vendor issued security updates addressing two critical vulnerabilities affecting the Windows version of the platform.

## #3

One of these vulnerabilities, identified as CVE-2023-41266 and categorized as a path traversal flaw, could be exploited to generate anonymous sessions and execute unauthorized HTTP requests. The second flaw, CVE-2023-41265, results in elevated privileges, and its initial fix was found to be inadequate, leading to the emergence of CVE-2023-48365.

## #4

In addition, the attackers executed multiple discovery commands, redirecting the output into .ttf files to obtain command output through path traversal. The threat actor employed various tactics to remain covert and gather information, including uninstalling antivirus software, altering the administrator password, and establishing an RDP tunnel using the Plink command-line connection tool.

## #5

In the concluding phase of the attack, the hackers deployed the Cactus ransomware on the compromised systems. Notably, Cactus ransomware actively exploits these vulnerabilities in publicly exposed Qlik Sense instances that have not been patched.

# Recommendations



**Immediate Patching:** Prioritize the prompt application of security updates and patches for Qlik Sense instances to address critical vulnerabilities and prevent potential exploits by Cactus ransomware.



**Anomaly Detection:** Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.



**Zero-Trust Architecture:** Consider adopting a zero-trust architecture, where no device or user is inherently trusted, and verification is required from everyone trying to access resources. This approach can limit the lateral movement within a compromised network.



**Backup and Recovery:** Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.



## Potential MITRE ATT&CK TTPs

<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation
<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0007</u></b> Discovery	<b><u>TA0008</u></b> Lateral Movement	<b><u>TA0011</u></b> Command and Control
<b><u>TA0010</u></b> Exfiltration	<b><u>T1657</u></b> Financial Theft	<b><u>T1018</u></b> Remote System Discovery	<b><u>T1059</u></b> Command and Scripting Interpreter
<b><u>T1053</u></b> Scheduled Task/Job	<b><u>T1053.005</u></b> Scheduled Task	<b><u>T1055</u></b> Process Injection	<b><u>T1059.001</u></b> PowerShell
<b><u>T1070.001</u></b> Clear Windows Event Logs	<b><u>T1083</u></b> File and Directory Discovery	<b><u>T1082</u></b> System Information Discovery	<b><u>T1071</u></b> Application Layer Protocol
<b><u>T1071.001</u></b> Web Protocols	<b><u>T1490</u></b> Inhibit System Recovery	<b><u>T1486</u></b> Data Encrypted for Impact	<b><u>T1659</u></b> Content Injection

# 🗡️ Indicators of Compromise (IOCs)

TYPE	VALUE
<b>IPv4</b>	45.61.147[.]176, 216.107.136[.]46, 144.172.122[.]30
<b>Domain</b>	zohoservice[.]net
<b>URLs</b>	hxxp[:]//zohoservice[.]net/putty[.]zip, hxxp[:]//216.107.136[.]46/Qlikensens_update[.]zip, hxxp[:]//216.107.136[.]46/Qlikensens_updated[.]zip, hxxp[:]//zohoservice[.]net/qlik-sens-Patch[.]zip, hxxp[:]//zohoservice[.]net/qlik-sens-nov[.]zip, hxxps[:]//download.anydesk.com/AnyDesk[.]exe
<b>File Paths</b>	C:\Users\Public\svchost.exe C:\windows\temp\file.exe C:\windows\temp\putty.exe C:\windows\temp\Qlikensens.exe C:\windows\temp\any.exe C:\temp\putty.exe C:\Windows\appcompat\AcRes.exe
<b>File Names</b>	file.exe, anydesk.zip, AcRes.exe, any.exe, putty.zip, Qlik_sense_enterprise.zip, qlik-sens-nov.zip, qlik-sens-Patch.zip, Qlikensens.exe, Qlikensens_updated.zip, Qlikensens_update.zip
<b>SHA256</b>	828e81aa16b2851561fff6d3127663ea2d1d68571f06cbd732fdf5672 086924d, 90b009b15eb1b5bc4a990ecdd86375fa25eaa67a8515ae6c6b3b5881 5d46fa82, 3ac8308a7378dfe047eacd393c861d32df34bb47535972eb0a35631a b964d14d, 6cb87cad36f56aefcefbe754605c00ac92e640857fd7ca5faab7b9542e f80c96

## Patch Details

Upgrade Qlik Sense Enterprise for Windows to a version that includes fixes, which are available in the following releases:

August 2023 Initial Release

May 2023 Patch 4

February 2023 Patch 8

November 2022 Patch 11

August 2022 Patch 13

Link:

<https://community.qlik.com/t5/Product-Downloads/tkb-p/Downloads>

## References

<https://www.arcticwolf.com/resources/blog/qlik-sense-exploited-in-cactus-ransomware-campaign/>

<https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801>

<https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2120325>

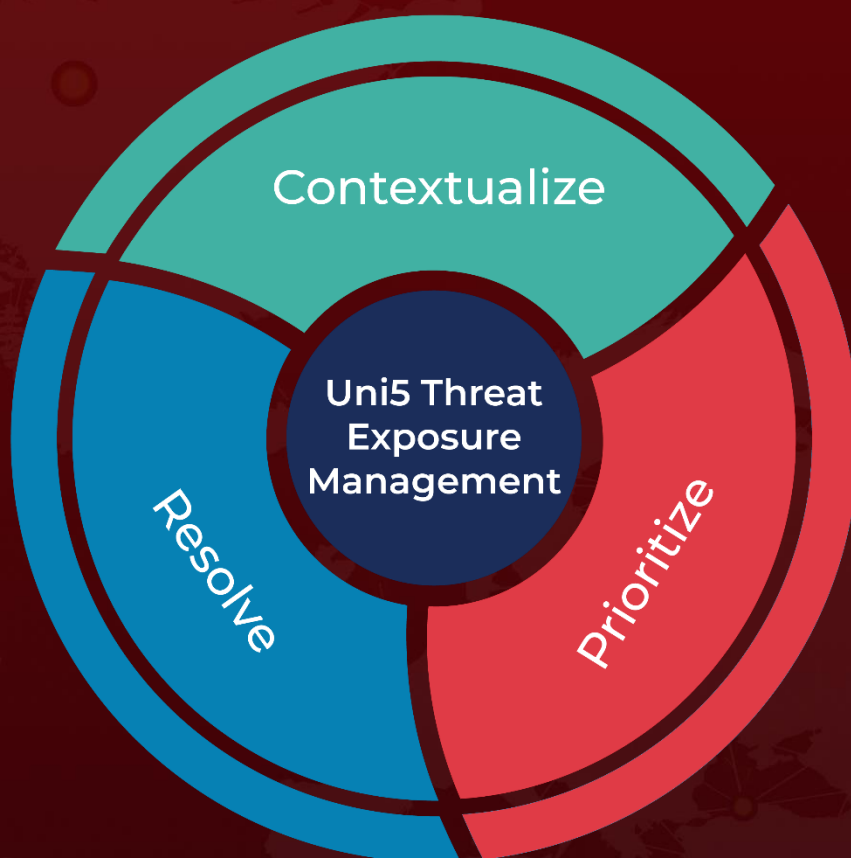
<https://www.hivepro.com/threat-advisory/cactus-ransomware-emerges-as-new-threat-targeting-large-enterprises/>



# 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

**December 1, 2023 • 04:30 AM**

© 2023 All Rights are Reserved by Hive Pro<sup>®</sup>



More at [www.hivepro.com](http://www.hivepro.com)