aDvens

Security for the greater good

Newscast

Critical vulnerability in Qlik

2023-12-04 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

Qlik

On 29 August 2023, Qlik published a security advisory in which the editor announced the discovery of two vulnerabilities: CVE-2023-41266 and CVE-2023-41265.

Then, on 20 September 2023, Qlik alert in a new security advisory concerning the partial correction of CVE-2023-41265 and the discovery of a new vulnerability (CVE-2023-48365).

Qlik Sense is a cloud-based analysis and business intelligence platform.

These three vulnerabilities are actively exploited by the Cactus ransomware group.

CVE-2023-41266

Improper validation over user-supplied data allows a remote, unauthenticated attacker to generate an anonymous session, enabling him to make HTTP requests to unauthorized access points.

Type of vulnerability

- CWE-20: Improper Input Validation

Risk

- Security policy bypass

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	Low
User Interaction	None	Impact on availability	None

Impacted Products

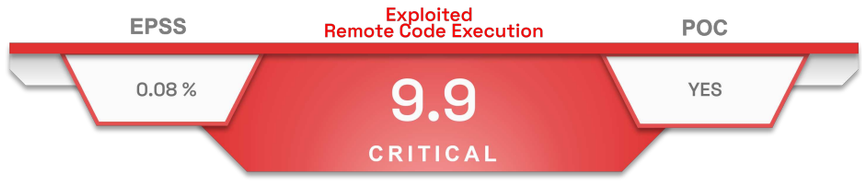
Versions Qlik Sense Entreprise for Windows environment:

- August 2022 Patch 12 and earlier
- November 2022 Patch 10 and earlier
- February 2023 Patch 7 and earlier
- May 2023 Patch 3 and earlier

Proof of concept

A proof of concept is available in open source.

CVE-2023-41265



An improper validation of HTTP Header in *Qlik Sense Entreprise* allows an authenticated attacker to communicate with application servers (backend) and elevate their privileges by sending specially crafted requests.

Joint exploitation of the CVE-2023-41265 and CVE-2023-41266 vulnerabilities would allow a remote, unauthenticated attacker to execute remote code.

Type of vulnerability

- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Risks

- Security policy bypass
- Privilege Escalation
- Remote Code Execution

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

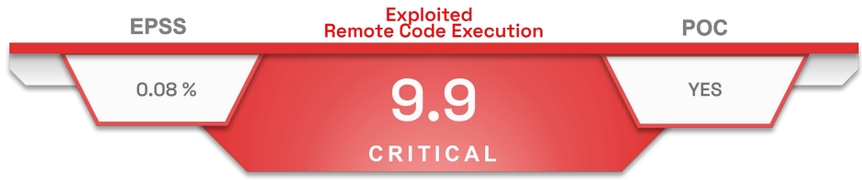
Versions Qlik Sense Entreprise for Windows environment:

- August 2022 Patch 12 and earlier
- November 2022 Patch 10 and earlier
- February 2023 Patch 7 and earlier
- May 2023 Patch 3 and earlier

Proof of concept

A proof of concept is available in open source.

CVE-2023-48365



An improper validation of HTTP Header in *Qlik Sense Entreprise* allows a remote attacker, via sending specially crafted request,to execute arbitrary code on the system with privileged rights.

Type of vulnerability

- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Risks

- Privilege Escalation
- Remote Code Execution

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

Versions Qlik Sense Entreprise for Windows environment:

- August 2023 Patch 1
- May 2023 Patch 5 and earlier
- February 2023 Patch 9 and earlier
- November 2022 Patch 11 and earlier
- August 2022 Patch 13 and earlier
- May 2022 Patch 15 and earlier
- February 2022 Patch 14 and earlier
- November 2021 Patch 16 and earlier

Recommendations

- Apply Patch 17 to Qlik Sense Entreprise for Windows version November 2021.
- Apply Patch 15 to Qlik Sense Entreprise for Windows version February 2022.
- Apply Patch 16 to Qlik Sense Entreprise for Windows version May 2022.
- Apply Patch 14 to Qlik Sense Entreprise for Windows version August 2022.
- Apply Patch 12 to Qlik Sense Entreprise for Windows version November 2022.
- Apply Patch 10 to Qlik Sense Entreprise for Windows version February 2023.
- Apply Patch 6 to Qlik Sense Entreprise for Windows version May 2023.
- Apply Patch 2 to Qlik Sense Entreprise for Windows version August 2023.

Further information is available in the editor's security advisory.

Proof of concept

A proof of concept is available in open source.

Indicators of compromise

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	IP	45.61.147[.]176	ManageEngine Server IP for zohoservice[.]net
TLP:CLEAR	IP	216.107.136[.]46	ManageEngine Server Hosting payload over HTTP
TLP:CLEAR	IP	144.172.122[.]30	ManageEngine Server Hosting payload over HTTP
TLP:CLEAR	Domain	zohoservice[.]net	Hosting payload over HTTP
TLP:CLEAR	URL	http[:]//zohoservice[.]net/putty.zip	Renamed PuTTY Link (Plink)
TLP:CLEAR	URL	http[:]//zohoservice[.]net/putty.zip	Renamed PuTTY Link (Plink)
TLP:CLEAR	URL	http[:]//216.107.136[.]46/Qliksens_update.zip	Renamed ManageEngine UEMS
TLP:CLEAR	URL	http[:]//216.107.136[.]46/Qliksens_updated.zip	Renamed ManageEngine UEMS
TLP:CLEAR	URL	http[:]//zohoservice[.]net/qlik-sens-Patch.zip	Renamed ManageEngine UEMS
TLP:CLEAR	URL	http[:]//zohoservice[.]net/qlik-sens-nov.zip	Renamed ManageEngine UEMS
TLP:CLEAR	File Path	C:\Users\Public\svchost.exe	Renamed Rclone
TLP:CLEAR	File Path	c:\windows\temp\file.exe	Renamed AnyDesk
TLP:CLEAR	File Path	c:\windows\temp\putty.exe	Renamed PuTTY Link (Plink)
TLP:CLEAR	File Path	c:\windows\temp\Qliksens.exe	Renamed ManageEngine UEMS
TLP:CLEAR	File Path	c:\windows\temp\any.exe	Renamed ManageEngine UEMS
TLP:CLEAR	File Path	C:\temp\putty.exe	Renamed PuTTY Link (Plink)
TLP:CLEAR	File Path	C:\Windows\appcompat\AcRes.exe	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	file.exe	Renamed AnyDesk Installer
TLP:CLEAR	Filename	anydesk.zip	Renamed AnyDesk Installer
TLP:CLEAR	Filename	AcRes.exe	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	any.exe	Renamed AnyDesk Installer
TLP:CLEAR	Filename	putty.zip	ZIP containing PuTTY Link (Plink)
TLP:CLEAR	Filename	Qlik_sense_enterprise.zip	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	qlik-sens-nov.zip	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	qlik-sens-Patch.zip	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	Qliksens.exe	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	Qliksens_updated.zip	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	Qliksens_update.zip	Renamed ManageEngine UEMS

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	SHA256	828e81aa16b2851561fff6d3127663ea2d1d68571f06cbd732fdf5672086924d	PuTTY Link (Plink)
TLP:CLEAR	SHA256	90b009b15eb1b5bc4a990ecdd86375fa25eaa67a8515ae6c6b3b58815d46fa82	ManageEngine UEMS Installer
TLP:CLEAR	SHA256	3ac8308a7378dfe047eacd393c861d32df34bb47535972eb0a35631ab964d14d	ManageEngine UEMS Installer
TLP:CLEAR	SHA256	6cb87cad36f56aefcefbe754605c00ac92e640857fd7ca5faab7b9542ef80c96	ManageEngine UEMS Installer

Sources

- https://arcticwolf.com/resources/blog/qlik-sense-exploited-in-cactus-ransomware-campaign/
- https://community.qlik.com/t5/Support-Updates/Qlik-Sense-Enterprise-for-Windows-New-Security-Patches-Available/ba-p/2108549
- 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/tac-p/2120510
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-48365
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41266
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41265