



# Qlik Sense HTTP Tunneling Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-41265
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-08-29 23:15:00 UTC
<b>Updated</b>	2023-09-08 13:59:00 UTC
<b>Description</b>	An HTTP Request Tunneling vulnerability found in Qlik Sense Enterprise for Windows for versions May 2023 Patch 3 and e

## Risk And Classification

**EPSS:** 0.925190000 probability, percentile 0.997350000 (date 2026-04-01)

**CISA KEV:** Listed on 2023-12-07; due 2023-12-28; ransomware use Known

**Problem Types:** CWE-444

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Qlik
<b>Product</b>	Sense
<b>Name</b>	Qlik Sense HTTP Tunneling Vulnerability
<b>Required Action</b>	Apply remediations or mitigations per vendor instructions or discontinue use of the product if remediation or mitigations are unavailable.
<b>Notes</b>	<a href="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/2110801</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2023-41265">https://nvd.nist.gov/vuln/detail/CVE-2023-41265</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	-	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_1	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_10	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_11	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_12	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_2	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_3	All	All

Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_4	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_5	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_6	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_7	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_8	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	august_2022	patch_9	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	february_2023	-	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	february_2023	patch_1	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	february_2023	patch_2	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	february_2023	patch_3	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	february_2023	patch_4	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	february_2023	patch_5	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	february_2023	patch_6	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	february_2023	patch_7	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	may_2023	-	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	may_2023	patch3	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	may_2023	patch_1	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	may_2023	patch_2	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	november_2022	-	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	november_2022	patch_1	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	november_2022	patch_10	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	november_2022	patch_2	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	november_2022	patch_3	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	november_2022	patch_4	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	november_2022	patch_5	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	november_2022	patch_6	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	november_2022	patch_7	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	november_2022	patch_8	All	All
Application	<a href="#">Qlik</a>	<a href="#">Qlik Sense</a>	november_2022	patch_9	All	All

## References

Reference	Source	Link	Tags
Release Notes   Qlik Community	MISC	<a href="https://community.qlik.com">community.qlik.com</a>	
Critical Security fixes for Qlik Sense Enterprise ... - Qlik Community - 2110801	MISC	<a href="https://community.qlik.com">community.qlik.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical

NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>	kev

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[379150](#) Qlik Sense Enterprise for Windows Remote Code Execution (RCE) Vulnerability (Authenticated)

[730994](#) Qlik Sense Enterprise for Windows Multiple Security Vulnerabilities

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)