full disclosure | zero day | 0-day | vision helpdesk | exploit

Critical Vulnerability in Vision Helpdesk Allows Unauthorized Session Access

Joel Aviad Ossi 02 November, 2024

What is Vision Helpdesk?

Vision Helpdesk is a helpdesk and customer support software designed to streamline support services for businesses by providing features such as ticket management, incident tracking, and customer service automation. It is used by

organizations worldwide, from startups to large enterprises, to efficiently manage and resolve customer queries. Vision Helpdesk's platform integrates various communication channels, making it an appealing solution for businesses of different sizes.

The Responsible Disclosure and Vendor Response

At WebSec B.V., we follow strict ethical guidelines when dealing with security vulnerabilities, ensuring that vendors are notified of any issues and given ample time to resolve them before we consider public disclosure. Our process began by submitting a critical vulnerability report to Vision Helpdesk regarding an Insecure Direct Object Reference (IDOR) vulnerability in their platform.

Timeline of Communication:

- **September 17 (Vendor)**:
  Vision Helpdesk responded to our initial vulnerability report, acknowledging receipt of our submission and informing us that they had forwarded the issue to their security team. The ticket was marked as critical.

- **September 21 (Vendor)**:
  The vendor's next response showed a misunderstanding of the issue. Instead of addressing the vulnerability in their code, they asked for access to a server where they believed our helpdesk was hosted. This indicated confusion, as the vulnerability was related to their product's software, not a specific server setup.

- **September 21 (WebSec)**:
  We responded promptly, clarifying that we were security researchers and did not operate a helpdesk. We reiterated that the issue was with their software, providing further details and asking them to address the vulnerability directly.

- **October 8 (WebSec)**:
  After waiting more than two weeks with no concrete follow-up from the vendor, we sent another message, explaining the severity of the vulnerability and setting a clear deadline of November 1, 2024, for the issue to be addressed. We warned that if no action was taken by this date, we would proceed with Full Disclosure to protect affected users ourselves.

- **Post-October 8**:
  Vision Helpdesk did not respond to any of our communications following October 8th. Despite the severity of the issue and the clear deadline set for resolution, they ceased all further communication.

With no response from the vendor by November 1st, we initiated the process of informing their clients directly.

- **Update: January 16, 2025**: Vendor confirmed the vulnerability and informed us that this was patched in version **5.6.10**

Escalation: Informing Vision Helpdesk's Clients and Moving Forward with CVE and Exploit-DB Submissions

After Vision Helpdesk missed the deadline of November 1, 2024, we escalated the situation. Using tools such as **Shodan.io** and Google Dorks, we identified several high-profile clients using the Vision Helpdesk platform who were likely vulnerable to the exploit. Among these clients were a large defense contractor and a prominent university.

We reached out to these clients directly, explaining the vulnerability and the potential risk. Two of these clients took immediate action to address the issue, although we are uncertain which client took which approach. One either completely removed the vulnerable script or implemented an IP whitelist to restrict access to the helpdesk platform, preventing unauthorized attempts to exploit the vulnerability.

Additionally, on **November 1**, we submitted a CVE request to **MITRE** to ensure the vulnerability is tracked and recognized by the global security community. Alongside this, we also submitted our Proof-of-Concept to **Exploit-DB**, providing the wider security community with the information needed to understand and remediate the vulnerability.

By **November 2**, we also released the Proof-of-Concept exploit on our GitHub page to enable users to test their own installations for this vulnerability.

The Impact: Reducing the Public Attack Surface

By reaching out to Vision Helpdesk's clients directly and submitting the vulnerability details to CVE, Exploit-DB, and GitHub, we believe that we were able to significantly reduce the public attack surface for this vulnerability. As organizations took the vulnerable system offline or implemented additional security controls, the chances of exploitation diminished. Now, with no resolution from the vendor, we are proceeding with full public disclosure of this vulnerability to spread awareness and help other users secure their systems.

The Technical Details: Serialized IDOR and Its Session Prediction Impact

Now, let's dive into the technical side of this vulnerability.

The core of this vulnerability lies in how Vision Helpdesk manages cookies, specifically the `` `vis_client_local` `` cookie. Normally, in web applications, cookies such as session IDs are created when a user authenticates to manage their session. However, in this case, the `` `vis_client_local` `` cookie could be generated without logging in.

Serialized IDOR

This vulnerability is a **Serialized IDOR** (Insecure Direct Object Reference). An **IDOR** vulnerability occurs when user input (in this case, the `vis_client_id`) can be modified to access unauthorized resources.

In Vision Helpdesk, the `vis_client_local` cookie is a serialized object encoded in Base64, containing user-specific attributes, including the `vis_client_id`, which uniquely identifies the user. The issue here is that the `vis_client_id` can be easily manipulated by an attacker.

1. **Cookie Structure**:
   The `vis_client_local` cookie is a Base64-encoded string representing a serialized object. This object contains user-specific attributes, such as the `vis_client_id`. The `vis_client_id` is a static field that identifies the current user in the system.

2. **Manipulating the Cookie**:
   By extracting and decoding the Base64-encoded string in the `vis_client_local` cookie, we were able to see the serialized object. The key field to exploit here was the `vis_client_id`.
   We then modified this value, incrementing or decrementing it by one to impersonate another user in the system. Once modified, we re-encoded the object back into Base64 and replaced the original `vis_client_local` value with the new one.

3. **Session Hijacking via Session Prediction**:
   The **impact** of this Serialized IDOR vulnerability is **Session Prediction**. By guessing or specifying valid `vis_client_id` values, an attacker can construct valid session tokens independently. This allows the attacker to directly impersonate other users without requiring their authentication, as the server interprets the modified `vis_client_local` cookie as a valid session.

> Unlike typical session management mechanisms that prevent predictable session identifiers, Vision Helpdesk's system permits an attacker to create a valid session solely by modifying the `vis_client_id` value. This effectively enables **Session Prediction**, allowing unauthorized access without user interaction.

This combination of **Serialized IDOR** and the **Session Prediction impact** increases the severity of the vulnerability, as it allows attackers to impersonate users without requiring authentication, posing a high security risk.

Download the Proof-of-Concept

To help system administrators and security teams verify if their version of Vision Helpdesk is vulnerable to this exploit, we have provided a downloadable **Proof-of-Concept** (PoC) script. You can use this script to test your installation and determine if it is affected by the **Serialized IDOR** vulnerability described in this article.

Download the Proof-of-Concept Script

Please use this PoC responsibly and only test systems you are authorized to assess. If your system is vulnerable, we strongly advise taking immediate action, such as disabling the affected script or implementing access control measures like an IP whitelist until the vendor releases a patch.

Conclusion: Moving Forward with Full Disclosure

With Vision Helpdesk failing to resolve the issue in a timely manner, and having already contacted affected clients, we feel it is necessary to move forward with full public disclosure of this vulnerability. We hope that by spreading awareness, other users of Vision Helpdesk will take steps to protect themselves from this serious flaw.

We strongly urge users of Vision Helpdesk to take immediate action—either by disabling the vulnerable script or by contacting the vendor to demand a fix.

At WebSec B.V., we remain committed to ethical hacking and responsible disclosure, and we hope this case serves as a reminder of the importance of security communication and rapid response to vulnerabilities.

Stay vigilant, stay secure.

*For more information or if you're interested in learning about the security of your applications, contact us via **websec.net/contact**. Learn more about our pentesting services to prevent vulnerabilities like these at **websec.net/services/pentesting**.*

Authored By Joel Aviad Ossi

Managing Director

Share with the world!

Need Security?

Are you really sure your organization is secure?

At WebSec we help you answer this question by performing advanced security assessments.

Want to know more? Schedule a call with one of our experts.

Schedule a call

About WebSec®

WebSec is a professional security firm offering a range of security services for companies of all sizes for the purpose of making you more cybersecurity resilient against the most modern cyber threats while remaining extremely cost-effective, flexible and high in quality.

Contacts

+1-307-316-8267

contact@websec.net

Location

Netherlands

Keurenplein 41, UNIT A6260

1069 CD, Amsterdam

United States

30 N Gould St # 39343

Sheridan, WY 82801

Navigate

Blog

Vacancies

VAPT Validation

Inquire

Solutions & Services

Penetration Testing

Red Teaming

Managed VDP

Security Staffing

Phishing Campaign

Security Subscriptions