Assetnote Identifies Critical Pre-Auth SQL Injection Vulnerability in Halo ITSM

Vulnerability could be exploited to read, modify, or insert data into critical IT support software

Assetnote - a Searchlight Cyber company

QUEENSLAND, AUSTRALIA, April 2, 2025 /EINPresswire.com/ -- - Assetnote, now a Searchlight Cyber company, has discovered a pre-authentication SQL injection vulnerability in the IT Support Management (ITSM) provider Halo.

This vulnerability is critical because of the nature of the data held within the software, which includes IT support tickets often containing credentials or internal documentation. Halo has issued a patch for the vulnerability following Assetnote's disclosure.

Assetnote investigated Halo ITSM after identifying it on its customers' attack surfaces to ensure that it couldn't be used as a point of compromise. There are currently around 1,000 cloud deployments of the software under the haloitsm.com domain, not accounting for on-premise deployments.

The researchers found that several areas of the code base are vulnerable to SQL injection, leading to a number of "close calls", which were only being prevented by using strongly typed objects enforcing the integer type. However, in the course of the investigation the team identified a pre-authentication SQL Injection vulnerability that an attacker could exploit to read, modify, or insert data inside the database connected to Halo ITSM. All of the technical details of the vulnerability can be found on the Assetnote Security Research blog.

Shubham Shah, SVP of Engineering and Research at Searchlight, explained the potential consequences of the vulnerability: "As an IT Support Management tool, Halo is often integrated with various internal and external systems and cloud providers, as well as containing sensitive information such as configuration files and credentials. This means that an attacker could have used this vulnerability to compromise any of the integrated systems, obtain sensitive data stored on the system, or even add themselves as an administrator and take over the instance."

The vulnerabilities identified by Assetnote have been patched in version 2.174.94, candidate

version 2.184.23, and beta version 2.186.2, and on-premise customers should upgrade urgently. As always, customers of the Assetnote Attack Surface Management platform were the first to know when this vulnerability affected them. Read the full Assetnote Security Research Center blog at https://slcyber.io/assetnote-security-research-center/loose-types-sink-ships-pre-authentication-sql-injection-in-halo-itsm/

About Assetnote, a Searchlight Cyber company:

Founded in 2018, Assetnote provides industry-leading attack surface management and adversarial exposure validation solutions, helping organizations identify and remediate security vulnerabilities before they can be exploited. Through continuous security testing and verification, Assetnote enables organizations to actionably defend their attack surface without noise.

Assetnote customers receive security alerts and mitigations at the same time to disclosure to third-party vendors. In January 2025, Assetnote was acquired by Searchlight Cyber. Combined, the companies form a holistic platform for combating external threats through Continuous Threat Exposure Management. Visit assetnote.io and slcyber.io for more information or Sonia Awan - PR for Assetnote at soniaawan@outbloompr.net

Sonia Awan
Outbloom Public Relations
soniaawan@outbloompr.net
Visit us on social media:
LinkedIn
