

# Knowledge Base



Created by Ian Batley on 4/17/2025 17:08  
Edited by Ian Batley on 4/25/2025 16:13

- security
- vulnerability
- cve

## Resolution

## General Information

This article contains frequently asked questions relating to the open redirect vulnerability affecting Halo versions up to 2.174.101 and all versions between 2.175.1 and 2.184.21.

A malformed link could allow the incorrect parsing of the returnurl parameter. If the user were to access this link, login to their account and then click on the incorrect returnurl link, the users tokens can be leaked.

## Are hosted Halo instances affected?

Hosted customers have been automatically updated to a patch to resolve this issue, and therefore no action is required by hosted customers. The patch was released on 2025-03-12 and hosted customers would have been upgraded shortly afterwards.

## Are on-premises Halo instances affected?

Halo on-premises installations should apply the latest stable or beta patch to their Halo instance to resolve this issue.

- Any patch >= 2.174.101.
- Any version >= 2.184.21.

## Next Steps

- > HaloCRM Guides
- > HaloITSM Guides
- > HaloPSA Academy
- > HaloPSA Website
- > Security

CORS Policy on Halo API

CVE-2023-44487 - HTTP/2 Rapid Reset Attack and the Halo Hosted Platform

CVE-2023-4863

CVE-2024-6200 - Stored Cross-Site Scripting in Tickets

CVE-2024-6201 - Emailing Template Injection

CVE-2024-6202 - SAML XML Signature Wrapping (XSW)

CVE-2024-6203 - Password Reset Poisoning

Data Storage And

01449 833111

support@imaginehalo.com

Language

English (United Kingd

▼