Liam B Follow
Oct 18, 2021 · 3 min read · Listen

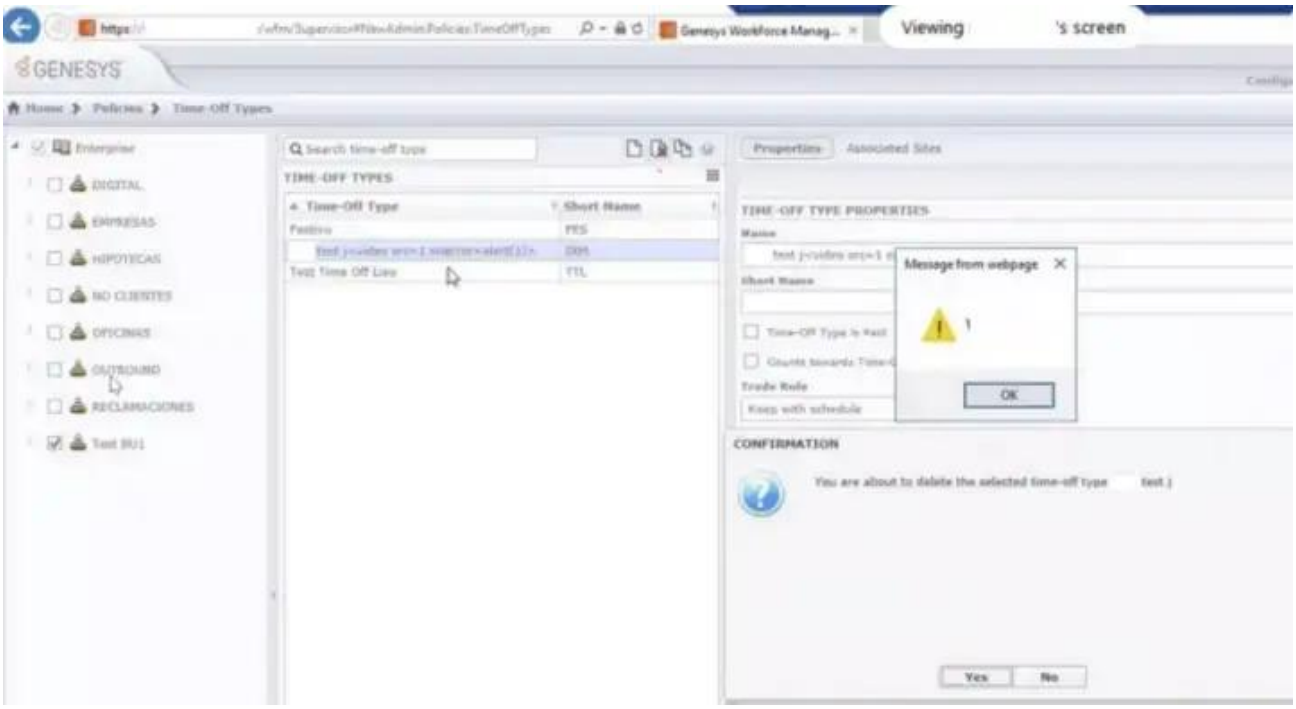
Cross Site Scripting Vulnerability within Genesys Workforce Management version 8.5.214.20

I identified this vulnerability over a year ago and due to multiple delays I have now only come around to submitting for a CVE. The job was performed while at work but checking with the client, they confirmed they were happy for me to report it as a CVE.

This issue was identified during a web application for a customer who was using the software provded by Genesys. It was a standard web application assessment that was performed over a number of days, however, it was performed over a Citrix session which is something that I never ever want to do again. I spent the time wondering if the client was watching my every move, as they had confirmed that they couldn't do any work anyway because I was essentially controlling their laptop! Not something I'd reccomend.

Onto the issue, the cross site scripting is a pretty standard one, while it didn't allow a standard script tag attack and it didn't pop off purely being input into fields, it was one that popped once the application tried to delete an entry that had been input into the system. The issue was originally identified within the Policies > Time-Off Types section of the application. Within this area it was possible to input holiday requests. JavaScript execution was confirmed by collection of the document.cookie flag. Further testing of this showed that it was in numerous places across the application and therefore appears to be an issue with the way the application as a whole. Unfortunately, timescales on the job did not allow for a full investigation on how or why the application was susceptible.

The payload used was <video src=1 onerror=alert(1)>



Confirmation of the XSS vulnerability

Confirmation of the version information

Information regarding the notification of of this to Genesys was originally started around July 2020. The following is a rough timeline of the steps taken to contact the vendor.

July 16th 2020 — Sent a DM to Genesys on Twitter regarding the issue identified

July 27th 2020 — No response so I left a comment on a Tweet about the DM. A response was provided via DM with an apology from Genesys and details around an internal contact to email about the issue.

July 28th 2020 — Sent an email to the internal contact detailing the issue.

August 10th 2020 — Sent a follow up email to internal contact asking for an update.

September 29th 2020 — Sent an follow up DM to the Twitter account asking if it could be chased

October 14th 2020 — I did get a response apologising and was provided with a contact form that I had previously filled in with no response.

Feb 2nd 2021 — Raised CVE Request

Sept 23rd 2021 — Request for more information from Mitre leading to this blog post.

Dec 15th 2021 — Assigned CVE-2021–26787