PHP2SHELL: CRITICAL RCE VULNERABILITY

Get the latest guidance →

CVE-2026-48558: SimpleHelp Authentication Bypass Indicators of Compromise

Zach Hanley | June 12, 2026 | Attack Blogs, Attack Research, Blogs, Disclosures

Intro

At Horizon3, we have been experimenting with generative AI heavily across all areas of work. One area I commonly work in is vulnerability research. Early in 2026, and inspired by DARPA's AIxCC, I ventured into creating an autonomous vulnerability research pipeline that would re-implement my research nerabilities. This internal own accord".

commercially relevant remote code execution, ver-side request forgery,

eline is software to analyze. Typically, I start my week by hunting down software of interest which

We Use Cookies

We use cookies to enhance your experience, understand website usage, and provide relevant content.

You can opt out of the sale or sharing of your personal information using the link below. For more information, please review our Privacy Policy.

Opt Out of Sale or Sharing of My Personal Information

focuses on enterprise software, commonly deployed software in our client base, and software that's historically been exploited in-the-wild and landed on the CISA Known Exploited Vulnerabilities (KEV) list.

We're no strangers to SimpleHelp, a remote monitoring and management application. In January 2025, we disclosed several critical vulnerabilities leading to SimpleHelp server compromise. One landed on CISA's KEV in May of 2025 and two more recently in April of 2026. This recent addition landed SimpleHelp back in our queue to look at again – this time by Sua Sponte.

And to our surprise, a few hours after ingesting the code into our pipeline, there was a finding! It's always a little hard to believe when the system reports a finding. Especially in code I know we've audited. But many ~~eyes~~ agents make light work, and we don't always get to comb through every line of code in a manual audit.

The Finding – CVE-2026-48558

SimpleHelp enables organizations to elect to use several authentication methods – one of which is OpenID Connect (OIDC). OIDC is very common to use in large enterprises where user management of the application is offloaded to an Identity Provider (IdP). One of the most common OIDC integrations supported is with Azure Active Directory (AD). SimpleHelp supports two flavors of OIDC: generic OIDC or specifically Azure AD OIDC.

The vulnerability identified affects servers configured to use either version of OIDC and is rooted in the way that SimpleHelp validates the IdP assertions. In many SimpleHelp deployments that have OIDC-type authentication enabled, an unauthenticated attacker can create and authenticate as a new "Technician" ed management activities scripts, and more.

orce MFA for technicians, m because on first login,

e to this technician

on provider is configured on the SimpleHelp server.

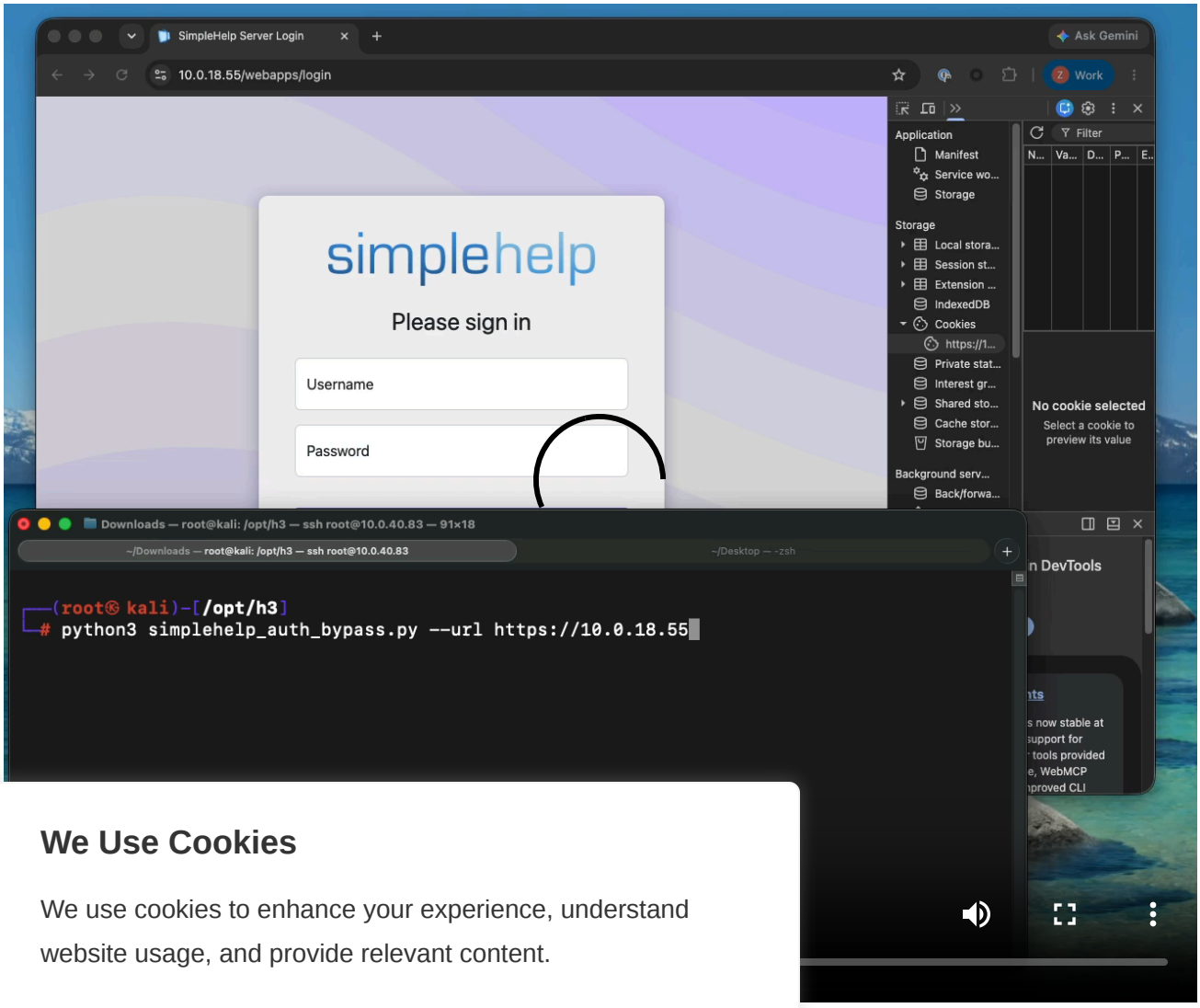
We Use Cookies

We use cookies to enhance your experience, understand website usage, and provide relevant content.

You can opt out of the sale or sharing of your personal information using the link below. For more information, please review our Privacy Policy.

2. A TechnicianGroup is associated with the OIDC provider – at least one TechnicianGroup has the OIDC provider enabled for it. This is a prerequisite for any OIDC login to function and is expected to be present in any deployment using OIDC authentication.
3. “Allow group authenticated logins” is enabled on the TechnicianGroup – this setting is found to be enabled in practice with the clients we assessed.

At this time, we will not be releasing any more technical details surrounding the vulnerability, but will detail the Indicators of Compromise that may be found if a server has been exploited via this vulnerability.



We Use Cookies

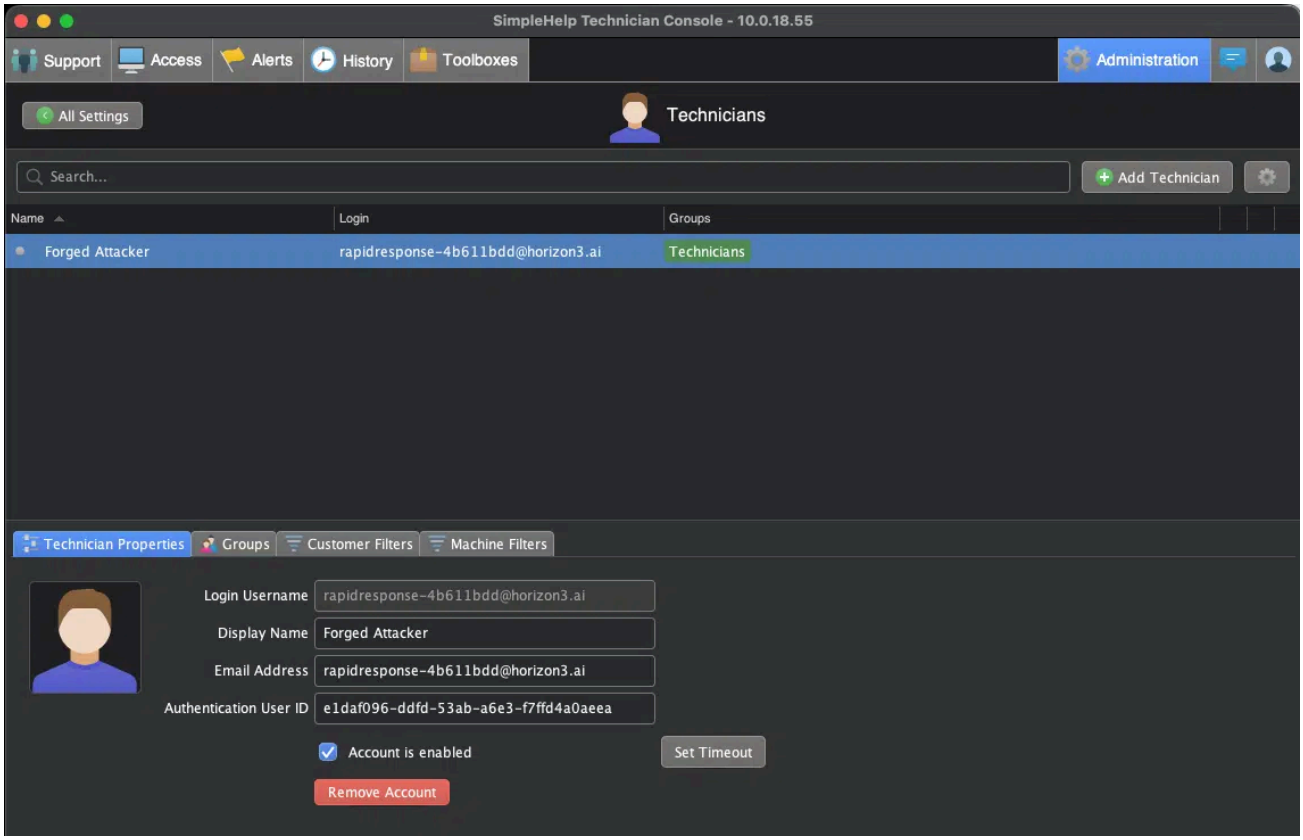
We use cookies to enhance your experience, understand website usage, and provide relevant content.

You can opt out of the sale or sharing of your personal information using the link below. For more information, please review our Privacy Policy.

technicians by navigating

Check “Show Group Authenticated Users”

Review the listed technicians for any unfamiliar technician names or email addresses.



The SimpleHelp application administrators can also view the server logs by navigating to:
`Administration -> Server Logs`

Analyze logs for unfamiliar technician names and email addresses

Registering technician login for `rapidresponse-4b611bdd@horizon3.ai / (Technicians)`

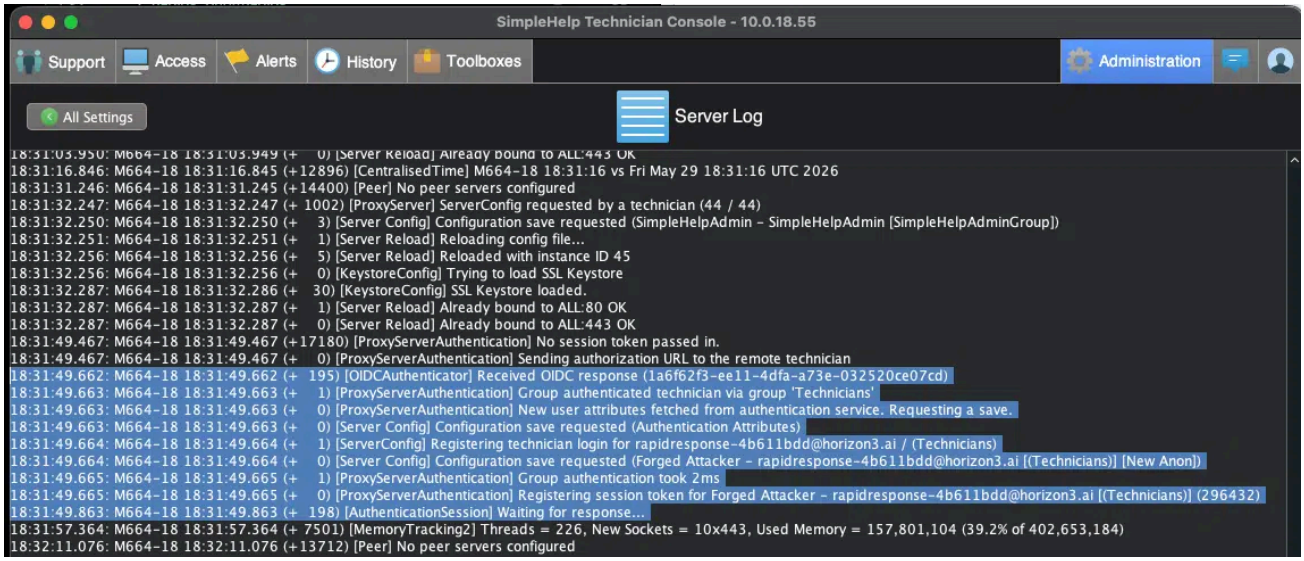
`apidresponse-`
`n])`

`.log`

We Use Cookies

We use cookies to enhance your experience, understand website usage, and provide relevant content.

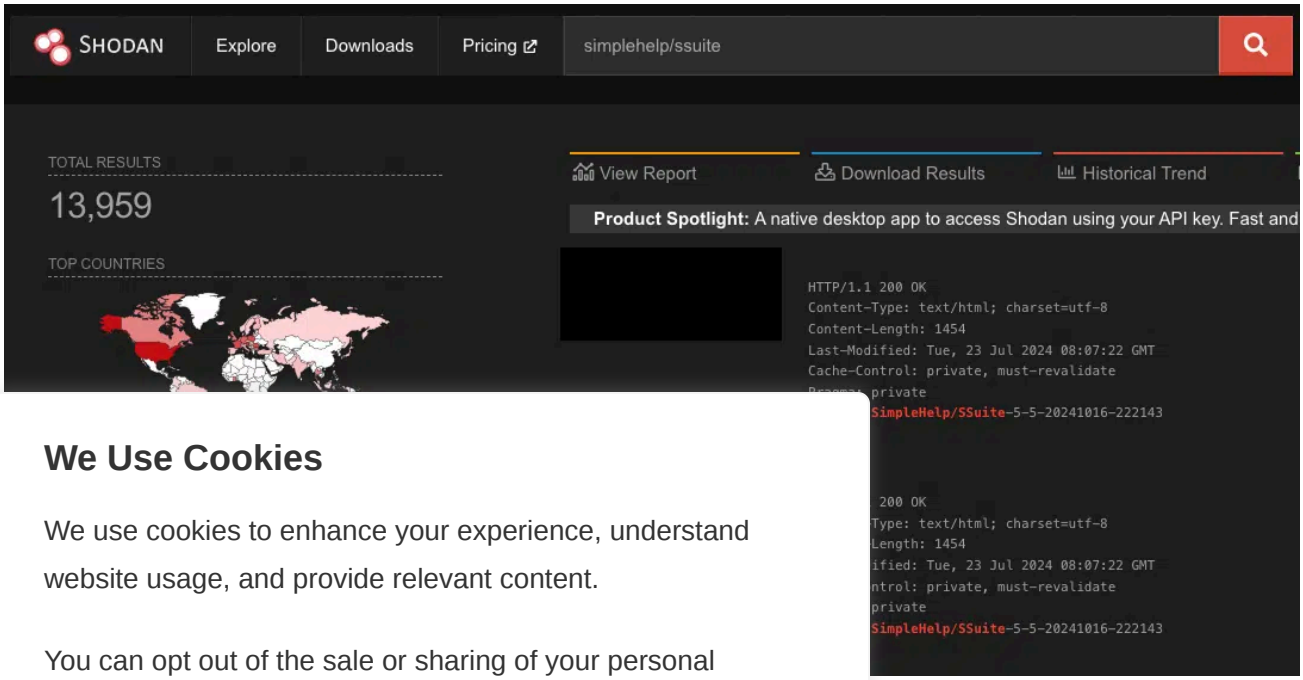
You can opt out of the sale or sharing of your personal information using the link below. For more information, please review our Privacy Policy.



Internet Exposure

Since our research in January 2025, which showed roughly 3,400 SimpleHelp servers exposed, that number has increased to nearly 14,000.

A random sampling of these servers indicated that roughly 7.2% of them were configured to use the vulnerable OIDC authentication method.



We Use Cookies

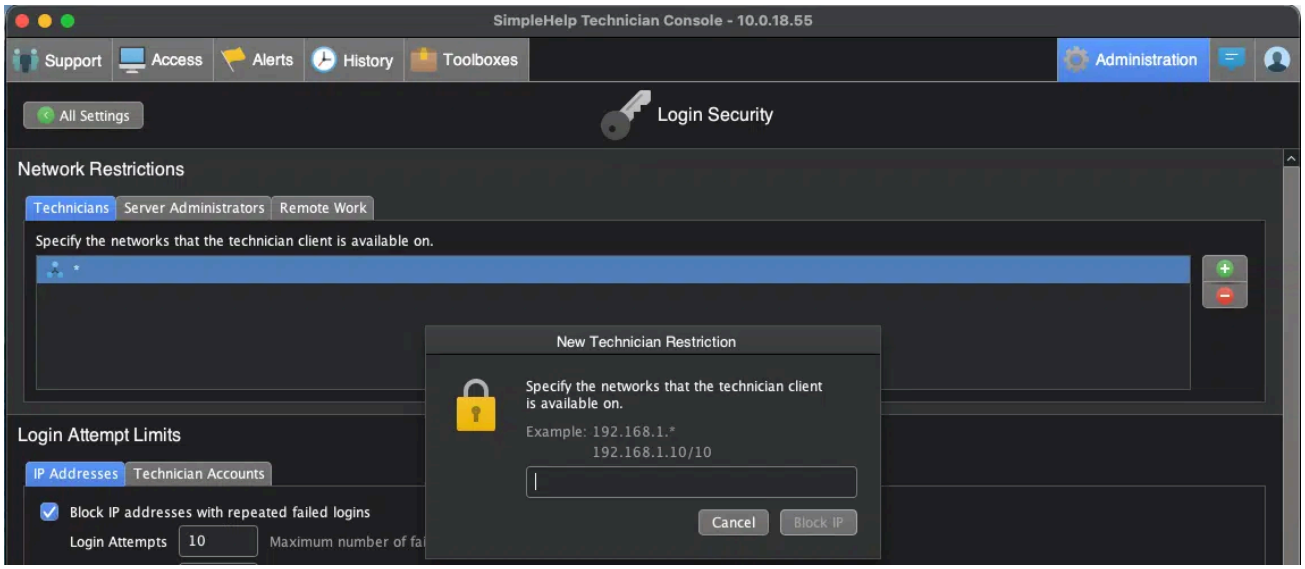
We use cookies to enhance your experience, understand website usage, and provide relevant content.

You can opt out of the sale or sharing of your personal information using the link below. For more information, please review our Privacy Policy.

While SimpleHelp does have optional configurations that support better locking down Technician login and authentication filters, we have not found them to be

enabled commonly in our client base.

If you cannot patch in a timely manner, consider applying IP restrictions to where Technicians can authenticate from in:
`Administration -> Login Security`



Disclosure Timeline

- **21 May 2026 –** Discovered authentication bypass now assigned CVE-2026-48558
- **21 May 2026 –** Validated the vulnerability was exploitable in real world conditions within our customer base and supplied mitigating controls
- **22 May 2026** – Reported issue to SimpleHelp
- **22 May 2026 – 1 June 2026** – We further communicate details of the vulnerability and determine exploitable configurations with SimpleHelp
- **9 June 2026** – We noticed that SimpleHelp has already released patches

We Use Cookies

We use cookies to enhance your experience, understand website usage, and provide relevant content.

You can opt out of the sale or sharing of your personal information using the link below. For more information, please review our Privacy Policy.

rity-update-2026-05

Let our experts walk you through a demonstration of NodeZero®, so you can see how to put it to work for your organization.

Get a Demo

Share:

HORIZON3

Contact us

Company

Solutions

Resources

We Use Cookies

We use cookies to enhance your experience, understand website usage, and provide relevant content.

You can opt out of the sale or sharing of your personal information using the link below. For more information, please review our Privacy Policy.

20 ell or Share My Personal Information