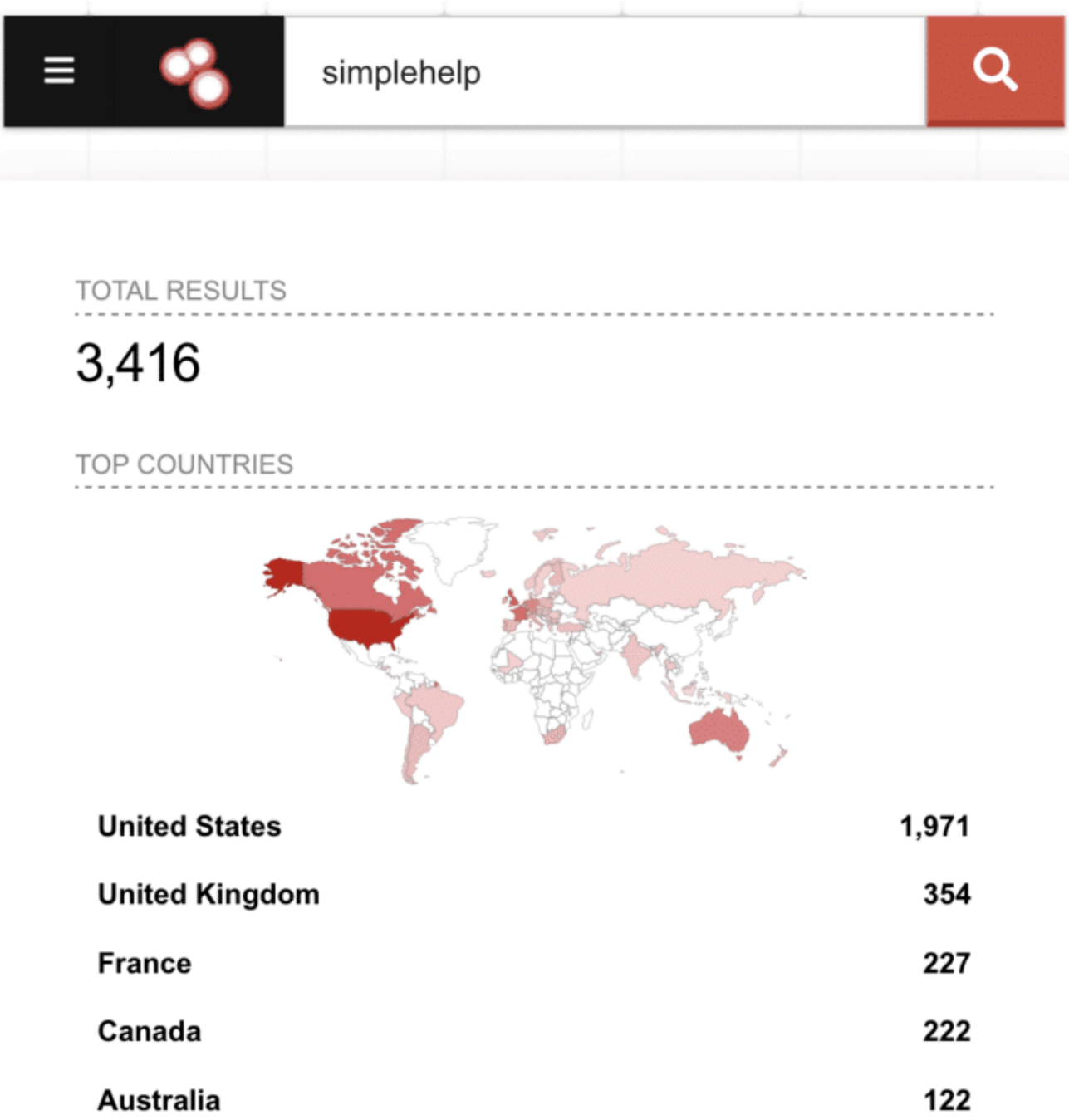
Critical Vulnerabilities in SimpleHelp Remote Support Software

Naveen Sunkavally | January 13, 2025 | Attack Blogs, Disclosures

Summary

2024 was bookended by notable zero-day vulnerabilities affecting popular remote support/access software: CVE-2024-1708 and CVE-2024-1709 affecting ConnectWise ScreenConnect and CVE-2024-12356 and CVE-2024-12686 affecting BeyondTrust products. These vulnerabilities were exploited in the wild and are on CISA's list of Known Exploited Vulnerabilities.

We were curious to see what other remote support software was out there and came across a tool called SimpleHelp. While we hadn't heard of it before, we found it being used by a number of our users, and it has a decent presence on the Internet.



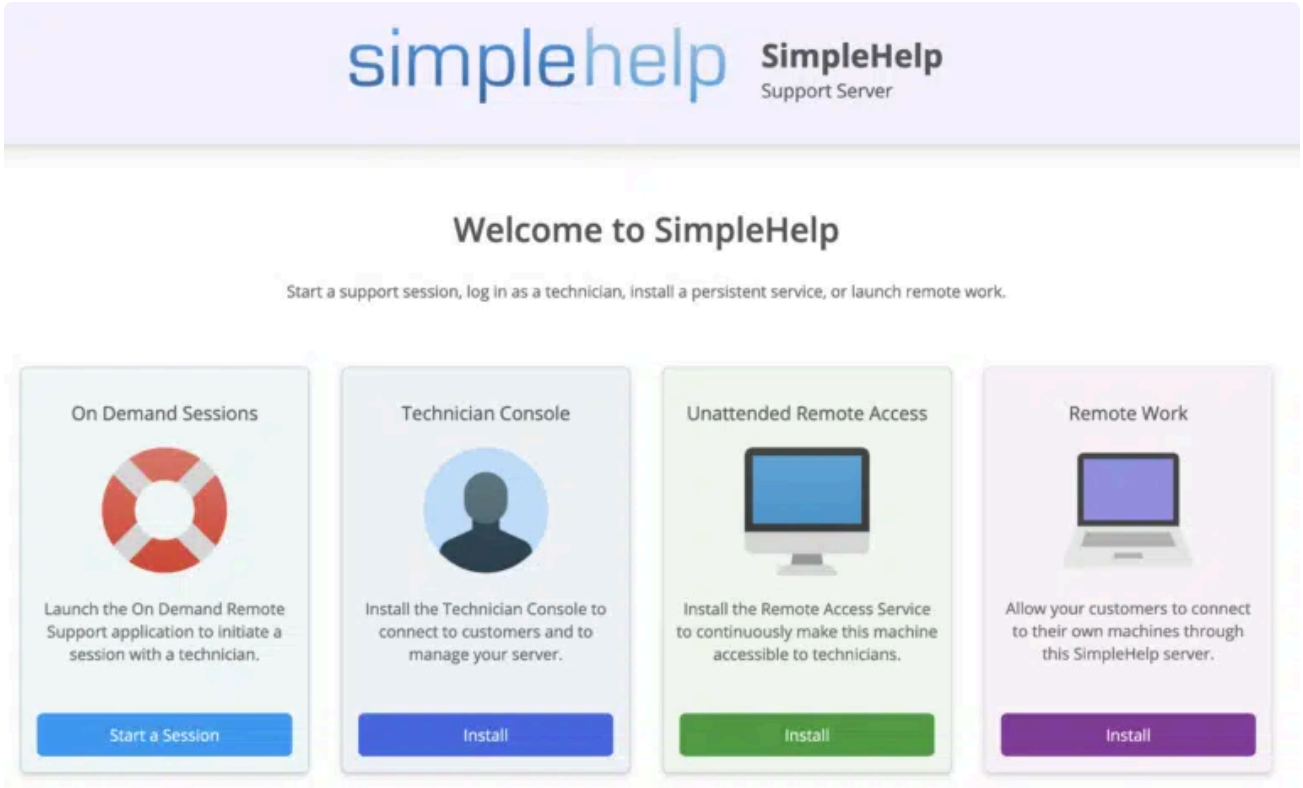
So we decided to “follow the data” and did a security audit of SimpleHelp. In our research, we uncovered three significant vulnerabilities that could be used to compromise a SimpleHelp server, as well as clients machines being managed by SimpleHelp. SimpleHelp quickly patched these vulnerabilities last week after our disclosure to their support team.

In this post we’ll cover the impact of the vulnerabilities we discovered, while withholding technical details to delay possible exploitation by script kiddies. The vulnerabilities are trivial to reverse and exploit though, and we encourage users to to upgrade ASAP to the latest SimpleHelp release, version 5.5.8 or 5.4.10 or 5.3.9 as of this writing.

Background

SimpleHelp has three primary personas: the administrator, the technician, and the customer.

- Administrators setup and configure the SimpleHelp server
- Technicians use SimpleHelp to connect to their customers who need remote support
- Customers are the ones asking for assistance



To get assistance, a customer first needs to download an executable from the SimpleHelp server and run it on their machine. To provide assistance, a technician needs to download a technican console executable from the SimpleHelp server and run it on their machine. The SimpleHelp server proxies communication between the technician and customer machines. SimpleHelp also supports an “unattended remote access” mode through which technicians can access customer machines without any customer interaction.

After installation, SimpleHelp is set up with a single admin account, `SimpleHelpAdmin`. This `SimpleHelpAdmin` can also serve as a technician. As a best practice, SimpleHelp encourages users to disable the `SimpleHelpAdmin` account and create separate technician accounts. It’s possible to then designate certain technicians as administrators using groups and permissions.

The SimpleHelp server is a really old school Java application. It can run on Windows, Linux, or macOS. The server acts as both a web application and a proxy server handling secure TCP or UDP connections initiated by technicians and customers. The proxy communication uses a custom messaging protocol.

CVE-2024-57727: Unauthenticated Path Traversal Vulnerability

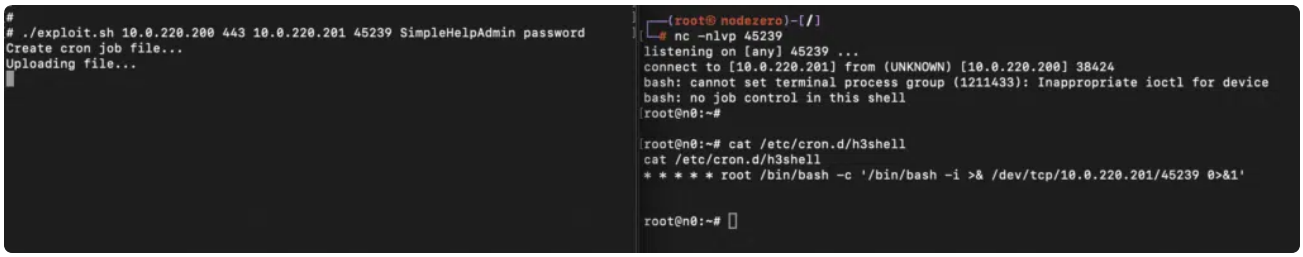
The first and most critical vulnerability we found is a path traversal vulnerability that enables unauthenticated attackers to download arbitrary files from the SimpleHelp server. This is bad because all SimpleHelp data is stored on disk as files. Logs and configuration secrets are encrypted but with a hardcoded key.

The most important SimpleHelp config file is `serverconfig.xml` in the `configuration` folder. It contains the hashed passwords for the `SimpleHelpAdmin` account and other local technician accounts. Depending on how SimpleHelp is configured, attackers can gain access to other types of secrets in various files such as LDAP credentials, OIDC client secrets, API keys, and TOTP seeds used for MFA.

CVSSv3 score: 7.5

CVE-2024-57728: Arbitrary File Upload to Remote Code Execution as Admin

If an attacker can login as the `SimpleHelpAdmin` user or as a technician with admin privileges, they can exploit a second vulnerability we found that allows for uploading arbitrary files to anywhere on the SimpleServer host. For Linux servers, an attacker could exploit this vulnerability to upload a crontab file to execute remote commands. For Windows servers, an attacker could overwrite executables or libraries used by SimpleHelp to get to remote code execution. Below is an example of landing a reverse shell on a Linux machine using a crontab file:



Admins also have the ability to interact with any connected customer machines or access customer machines directly if unattended access is configured.

CVSSv3 Score: 7.2

CVE-2024-57726: Privilege Escalation From Technician to Server Admin

If an attacker gains access as a low-privilege technician, there is a path for that technician to elevate their privileges to that of an admin. This is because of a third vulnerability we found where some admin functions in SimpleHelp were missing backend authorization checks. Through a crafted sequence of network calls, a technician can promote themselves to an admin. Once a technician becomes an admin, they can exploit the previous arbitrary file upload vulnerability to take over the SimpleHelp server.

The CVSS score for this vulnerability takes into account a “scope change” because an admin user can potentially access connected client machines that the low privilege technician did not have access to.

CVSSv3 Score: 9.9

Detection

The version of a SimpleHelp server can be determined from accessing the `/allversions` endpoint or inspecting the HTTP `Server` header. Any version less than 5.5.8 or 5.4.10 or 5.3.9 (any build before 2025) is highly likely to be exploitable.

```
# curl -k https://10.0.229.6/allversions
SH Version:             SSuite-5-5-20241016-222143
Visual Version:         5.5.7
Access Version:         00110278455 (Wed, 16 Oct 2024 21:23:40 GMT)
Customer Version:       00110278454 (Wed, 16 Oct 2024 21:23:36 GMT)
Technician Version:     00110278458 (Wed, 16 Oct 2024 21:23:52 GMT)
Remote Work Version:    00110278458 (Wed, 16 Oct 2024 21:23:52 GMT)
Present Version:        00110278458 (Wed, 16 Oct 2024 21:23:52 GMT)
Group Access Version:   00110278458 (Wed, 16 Oct 2024 21:23:52 GMT)
#
```

Remediation

We urge all users of SimpleHelp to upgrade ASAP to the latest patch version 5.5.8/5.4.10/5.3.9. SimpleHelp published a KnowledgeBase article here with more information.

Note that SimpleHelp, like other remote access tools, is a tool that has been known to have been abused by threat actors. There's a chance the vulnerabilities disclosed here are already well known.

Timeline

- **Dec. 30, 2024**: Horizon3.ai contacts SimpleHelp to ask for a security contact
- **Jan. 6, 2025**: Horizon3.ai gets security contact from SimpleHelp and discloses vulnerabilities
- **Jan. 7, 2025:** As part of its rapid response program, Horizon3.ai notifies affected customers who are exploitable to these vulnerabilities
- **Jan. 8, 2025**: SimpleHelp releases patch version 5.5.8 and 5.4.10.
- **Jan. 13, 2025**: SimpleHelp releases patch version 5.3.9.
- **Jan. 14, 2025**: CVEs assigned

References

- SimpleHelp KB Article
- CVE-2024-57726
- CVE-2024-57727
- CVE-2024-57728