Security Vulnerabilities in SimpleHelp 5.5.7 and earlier

Please make sure you read this guide fully before patching your SimpleHelp installation.

SimpleHelp versions 5.5.7 and all earlier releases are vulnerable to a set of security exploits (published under CVE-2024-57726, CVE-2024-57727 and CVE-2024-57728).

This Knowledge Base article discusses the impact of these security vulnerabilities, and the steps customers can take to secure SimpleHelp.

Updates

- (12/01/2025) Added 5.3.9 patch, and password reset instructions.
- (31/01/2025) Reissued 5.4.10 patch, to fix Let's Encrypt certificate challenges being blocked.
- (03/02/2025) Additional details and steps added
- (12/02/2025) CVEs listed

Suggested Action Summary

These exploits are severe. Please upgrade or patch your SimpleHelp version to a secure release as soon as possible.

See the [illegible] for the characteristics of Compromised Instances.

Join our mailing list to receive security announcements and update release notes. Log into your account on our site (at https://simple-help.com/account), go to the Privacy tab and activate the toggle next to Mailing List.

Steps to Secure SimpleHelp

The easiest method to prevent malicious exploitation is to upgrade your SimpleHelp server as soon as possible.

- **SimpleHelp v5.5 Users** - SimpleHelp v5.5.8 and later versions resolve these vulnerabilities. The latest release is available on our Download Page.
- **SimpleHelp v5.4 Users** - A patch for SimpleHelp **v5.4.10** is now available. Instructions for downloading and applying this patch are detailed below.
- **SimpleHelp v5.3 Users** - A patch for SimpleHelp **v5.3.9** is now available. Instructions for downloading and applying this patch are detailed below.

As it is possible that a server's configuration file could have been exposed we recommend taking these additional steps:

- Change the Administrator password of the SimpleHelp server. See Administration Guide for details.
- Change the passwords for Technician accounts, where the technician's do not log in using a third party authentication service like Active Directory. See Administration Guide for details.
- Restrict the IP addresses that the SimpleHelp server can expect Technician and Administrator logins from, where possible. See Login Restrictions for details.

UPGRADING TO V5.5.8 OR LATER

Please make sure you read the Steps to Secure SimpleHelp section above.

Download and install the latest release on our Download Page for your server platform.

- **Windows** Download and run the server installer on your SimpleHelp server. The server will automatically update and your configuration will be preserved.
- **Linux** We suggest using the Linux Installation Script to easily upgrade your Linux SimpleHelp instance.

If you access the **/allversions** page of your SimpleHelp server you will see the server version listed:

```
Visual Version:      5.5.8
```

PATCHING V5.4.10

Please make sure you read the Steps to Secure SimpleHelp section above.

This patch is specifically for customers running v5.4.10. The steps to apply the patch are as follows:

1. Stop your SimpleHelp server instance.
   - On Windows stop the **SimpleHelp Server** Windows service.
   - On Linux, run the **serverstop.sh** script.
2. In your SimpleHelp server's installation location, overwrite the file **lib/shelp-jar-with-dependencies.jar** with this version (the SHA1 digest of this file is b83006f0ddf4439623d4f8015bbcadda45f9475b).
3. Start your SimpleHelp server instance.

To verify the patch has been applied, check the server's log for the Patch line:

```
[SimpleHelp] Server Version v5.4.10
...
[SimpleHelp] Patch 070125
```

PATCHING V5.3.9

Please make sure you read the Steps to Secure SimpleHelp section above.

This patch is specifically for customers running v5.3.9. The steps to apply the patch are as follows:

1. Stop your SimpleHelp server instance.
   - On Windows stop the **SimpleHelp Server** Windows service.
   - On Linux, run the **serverstop.sh** script.
2. In your SimpleHelp server's installation location, overwrite the files (secure_utils.jar, secure_nlink.jar, secure_shelp.jar) in the **lib** directory with this version (the SHA1 digest of this ZIP is c490c1d715bac726d2414022c7d9afef5534566d).
3. Start your SimpleHelp server instance.

To verify the patch has been applied, check the server's log for the Patch line:

```
[SimpleHelp] Server Version v5.3.9
...
[SimpleHelp] Patch 070125
```

The characteristics of compromise depend on how your SimpleHelp server was configured. In the worst case, with permissive settings, these vulnerabilities could allow an attacker to:

- Retrieve the server's configuration file, exposing technician account information and password hashes.
- Exploit weak passwords on the server for accounts configured to allow local technician access.
- Log into your SimpleHelp instance, potentially with SimpleHelp administrator Technician privileges, allowing them to reconfigure the server.
- Gain remote administrator system/root access to registered machines. This could for instance allow them to:
    - Reconfigure Access services to point to a SimpleHelp server they control.
    - Install other software or malware on the machine.
    - Access data on the machine.

- Retrieve files from known locations on the SimpleHelp server host, outside of the SimpleHelp installation directory.
- A malicious user that has technician access to a SimpleHelp instance can use a customised sequence of Technician Console commands to write data on the server outside of expected data storage locations.

Characteristics of Compromise

An attack would likely first exploit the SimpleHelp server, and then use the server to compromise endpoints that are registering with the SimpleHelp server.

SERVER COMPROMISE

- A server that was not restarted during the potential compromise timeline, and had no technician logins during this time, is expected to not be compromised. Remedial action should still be taken to ensure server security.
- A server accepting logins from approved IP addresses only, or servers that are not publicly accessible, are unlikely to be compromised by third parties.
- A server with the following is expected to not be compromised:
    - SimpleHelpAdmin disabled, and
    - technician account local logins disabled, with all authentication going through an authentication service such as LDAP or Active Directory).

- Compromised servers may exhibit any of the following:
    - Technician logins from unexpected locations / IP addresses (assuming IP restrictions were not in place).
        - The server log will include this information. The following log sequence highlights the username and remote IP address.
        - [Authentication] Valid tech connection attempt username with password, checking credentials...[ProxyServer] Incoming IP identified as 10.x.x.x
        - Server Event alerts configured for Technician Logins will fire with this information.

    - The History tab may show unrecognised sessions.
        - A compromised Technician account could affect remote machines outside of sessions (e.g. using a Toolbox or a Monitoring Alert, see the technician guide).

    - A server with unexpected API tokens, or lacking API IP restrictions.

NOTE: As of 5.5.8, any "[WebDownloadServer] Insecure request..." log entries indicate that a remote client is performing a check on your server for an unauthorised resource.

REMOTE MACHINE COMPROMISE

Endpoints cannot have been compromised through SimpleHelp in these circumstances:

- Machines that have been offline, or last registered before the date of compromise
- Services that do not have scripting or monitoring permissions enabled, and have a password set

Endpoints may have been compromised if:

- An endpoint showing changes to serviceconfig.xml during the compromise timeline should be checked to ensure that there are no unauthorised registration URLs in the serviceconfig.xml
    - Any unrecognised URLs set in the server addresses list in your Remote Access services' configuration would strongly indicate malicious activity. If you notice or suspect a Remote Access service's configuration has been tampered with, Stop the service or uninstall it, isolate the machine and get specialist advice
    - The last modified time of the service configuration will give an indication as to whether the service's configuration was altered. If it was not altered, then all malicious activity would need to occur through your SimpleHelp server, and not through a third party server

- Remote Access Session logs, in the service's logs directory, connecting to unauthorised server URLs
- Unexpected outgoing connections from the endpoints to unauthorised IP addresses

COMPROMISE ENDPOINT ACTIONS

If you notice any of the following indicators of compromise or have reason to suspect your server or machines have been affected:

- Isolate the affected machines.
- Terminate the Remote Access Service process and startup service/daemon (You can use the Stop button in the configurer, see: https://simple-help.com/remote-access-guide#registration-details)
- Take a backup of the service's logs directory: https://simple-help.com/kb---locating-the-remote-access-service-installation-folder#locating-service-logs
- Share your Remote Access Service logs with SimpleHelp (contact@simple-help.com) for review
- Uninstall the Remote Access Service
- Seek advice from security specialists and contact appropriate authorities for endpoint security

- Change the passwords for Technician accounts, where the technicians are permitted to log in using server credentials
  - Our suggestion is to entirely disable local Technician account logins, and to only allow authentication using an authentication service like Active Directory, LDAP etc

- Create new API tokens, if in use
- Restrict the IP addresses that the SimpleHelp server can expect Technician and Administrator logins from
- Restrict the IP addresses from which clients can perform API requests (if any)
- Restrict the IP addresses, on the firewall, from which the SimpleHelp server can accept connections from
- Create Server Event alerts for the following so that administrators are notified of server access:
  - Administrator logins
  - Failed login attempts
  - Configuration changes

- Check whether any Remote Access Services have been reconfigured to include an unrecognised server URL. Version 5.5.9 contains the Configuration Analysis tool to make this easier

Join our mailing list to receive security announcements and update release notes. Log into your account on our site (at https://simple-help.com/account), go to the Privacy tab and activate the toggle next to Mailing List.

Send us your Questions

Please Contact Us with any queries, or if you need more information.