Bria...
@bri...

GoAnywhere MFT, a popular file transfer application, is warning about a zero-day remote code injection exploit. The company said it has temporarily implemented a service outage in response.

I had to create an account on the service to find this security advisory, so I'll just paste the advisory here:

"On Prem

Create account Login

n/Technical BulletinFeb 1, 2023

A Zero-Day Remote Code Injection exploit was identified in GoAnywhere MFT. The attack vector of this exploit requires access to the administrative console of the application, which in most cases is accessible only from within a private company network, through VPN, or by allow-listed IP addresses (when running in

Create account Login

nts, such as Azure or AWS).

If the administrative console is exposed to the public internet, it is highly recommended partnering with our customer support team to put in place appropriate access controls to limit trusted sources.

The Web Client interface, which is normally accessible from the public internet, is not susceptible to this

Create account Login

administrative interface.

If your administrative interface had been publicly exposed and/or appropriate access controls cannot be applied to this interface, follow these steps to evaluate and mitigate your exposure:

1. Review all administrator users

Evaluate your admin user accounts for anything suspicious.

Create account Login

on these accounts include:

Unrecognized usernames

You can view more details by clicking the cog icon next to any User Name listed and selecting the “View” option.

The Created By details show ‘system’

Note: There are some default, or initial admin user accounts that are created automatically - either through initial

Create account Login

default ‘disabled’ root and administrator accounts. If there are admin accounts created by ‘system’ that aren’t recognized, investigate further.

The timing of the account creation is suspicious

The Created On time and date may not be during a time when you would have been working with the platform.

Admin Audit Log shows a

Create account Login

disabled super user creating this account

Search the Administration log for activity (Reporting -> Audit Logs -> Administration). Search for anything created by root user.

Click the magnifying glass next to the log of suspicious activity to view more details.

2. Apply mitigation configuration

On the file system where GoAnywher

Create account Login

edit the file [install_dir]/adminroot/WEB_INF/web.xml

Find and remove (delete or comment out) the following servlet and servlet-mapping configuration in the screenshot below.

Before:

<servlet>

<servlet-name>License Response Servlet</servlet-name>

<servlet-class>com.linoma.ga.ui.admin.servlet.LicenseResponseServlet</servlet-class>

Create account Login

<load-on-startup>0</load-on-startup>

</servlet>

<servlet-mapping>

<servlet-name>Licenses Response Servlet</servlet-name>

<url-pattern>/lic/accept/</url-pattern>

After:

<!--

Add these tags to comment out the following section (as shown) or simply delete this section if you are not familiar

Create account Login

```
<servlet>

    <servlet-name>License Response Servlet</servlet-name>

    <servlet-class>com.linoma.ga.ui.admin.servlet.LicenseResponseServlet</servlet-class>

    <load-on-startup>0</load-on-startup>

</servlet>

<servlet-mapping>

    <servlet-name>Licenses Response Servlet</servlet-name>

    <url-pattern>/lic
```

Create account Login

</servlet-mapping>

-->

Restart the GoAnywhere MFT application

If GoAnywhere MFT is clustered, this change needs to happen on every instance node in the cluster.

If you have questions, our support team is here to help. Please contact Support via the portal my.goanywhere.com/, email goanywhere.support@helpsystem

Create account Login

944-4242 for assistance. "

Feb 02, 2023, 02:53 PM

45 boosts · **0** q

EN

BTW, the fact that I can copy past a an entir e secu rity advis ory of this lengt h in one post is one of the

Create account Login

reasons I love posting here.

1

EN

@briankrebs

One of GoAnywhere's customers, listed on their website, is McKesson.

"The CDC and HHS selected McKesson as the U.S. government's

Create account Login

d distributor for Covid-19 vaccine doses and ancillary supply kits under Operation Warp Speed."

Security comedy meets pandemic.

0

EN

@briankrebs They may not talk abou

Create account Login

cly, but I'm told that Informatica MFT uses GoAnywhere under the hood.

0

EN

@briankrebs goanywhere.support@helpsystems.com … Is that the same helpsystems I'm thinking of?

Create account Login

0

EN

@briankrebs This is actually pre-auth RCE, 100% confirmed and their advisory sucks. Good luck to their customers!

1+

EN

@stevenseeley @bri

Create account Login

ssiTheDog Yep.. infosec.exchange/@frycos/10979…

0

EN

@stevenseeley may be they were referring to the advisory as requiring authentication

1

EN

@hamisec 🤔

0

Create account Login

EN

@briankrebs Thanks for posting this. We get pretty comprehensive vulnerability advisories but this one didn't come from our MSSP.

So, you can count at least one more org patc

Create account Login

to a Mastodon post...

1

EN

@briankrebs Follow-up, you're quoted in a Rapid7 Emergent Threat advisory that just went out with their article by Caitlin Condon today. rapid7.com/blog/p

Create account Login

02/0
…

0

EN

@bri
ankr
ebs

It's
nice
to
have
a
train
of
thou
ght,
inde
ed.

A
lost
skill

Create account Login