

[←](#) [P...](#) 



Bria...
[@bri...](#)

GoAnywher
e MFT, a
popular file
transfer
application,
is warning
about a
zero-day
remote
code
injection
exploit. The
company
said it has
temporarily
implement
ed 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 Prom

Create account

Login



n/Technica l 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 administrative users

Evaluate your admin user accounts for anything suspicious.

[Create account](#)[Login](#)

on these
accounts
include:

Unrecogniz
ed
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
automatica
lly - either
through
initial

[Create account](#)[Login](#)

default
'disabled'
root and
administrat
or
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
Administra
tion log for
activity
(Reporting
-> Audit
Logs ->
Administra
tion).
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
configurati
on

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
configurati
on in the
screenshot
below.

Before:

```
<servlet>
```

```
    <servlet-  
name>Lice  
nse  
Response  
Servlet</se  
rvlet-  
name>
```

```
    <servlet-  
class>com.  
linoma.ga.  
ui.admin.se  
rvlet.Licens  
eResponse  
Servlet</se  
rvlet-class>
```

[Create account](#)[Login](#)


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

```
</servlet>
```

```
<servlet-  
mapping>
```

```
<servlet-  
name>License  
Response  
Servlet</se  
rvlet-  
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>Lice
nse
Response
Servlet</se
rvlet-
name>

    <servlet-
class>com.
linoma.ga.
ui.admin.se
rvlet.Licens
eResponse
Servlet</se
rvlet-class>

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

</servlet>

<servlet-
mapping>

    <servlet-
name>Lice
nses
Response
Servlet</se
rvlet-
name>

    <url-
pattern>/lic
```

[Create account](#)[Login](#)

```
</servlet-  
mapping>
```

```
-->
```

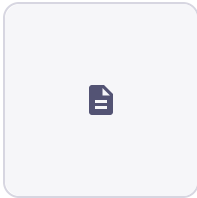
Restart
the
GoAnywh
e MFT
application

If
GoAnywh
e 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.goanyw
here.com/](https://my.goanywhere.com/),
email
goanywh
e.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

reas
ons I
love
posti
ng
here.

↩ 1



EN  

@bri
ankr
ebs

One
of
GoA
nywh
ere's
cust
omer
s,
liste
d on
their
webs
ite, is
McK
esso
n.

"The
CDC
and
HHS
selec
ted
McK
esso
n as
the
U.S.
gove
rnme
nt's

Create account

Login

d
distri
butor
for
Covi
d-19
vacci
ne
dose
s
and
ancill
ary
supp
ly
kits
unde
r
Oper
ation
Warp
Spee
d."

Secu
rity
com
edy
meet
s
pand
emic
.

↩ 0



EN 🗨 🌐

@bri
ankr
ebs
They
may
not
talk
abou

Create account

Login

cly,
but
I'm
told
that
Infor
mati
ca
MFT
uses
GoA
nywh
ere
unde
r the
hood
.

↩ 0



EN

@bri
ankr
ebs
goan
ywhe
re.su
pport
@hel
psyst
ems.
com
...
Is
that
the
sam
e
helps
yste
ms
I'm
think
ing
of?

Create account

Login

 0

EN   

@bri
ankr
ebs

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




 1+

 EN  

@ste
vens
eeley
@bri

Create account

Login

https://infosec.exchange/@briankrebs/109795710941843934

16/20

ssiT
heDo
g
Yep..
infos
ec.ex
chan
ge/@
fryco
s/10
979...
0

EN  

@ste
vens
eeley
may
be
they
were
referr
ing
to
the
advis
ory
as
requi
ring
auth
entic
ation
1

EN  

@ha
mise
c 
0

Create account

Login



EN  

@bri
ankr
ebs
Than
ks
for
posti
ng
this.
We
get
prett
y
com
preh
ensiv
e
vulne
rabili
ty
advis
ories
but
this
one
didn't
com
e
from
our
MSS
P.

So,
you
can
coun
t at
least
one
more
org
patc

Create account

Login

to a
Mast
odon
post.

..

↩ 1

EN   

[@bri
ankr
ebs](#)

Follo
w-up,
you'r
e

quot
ed in

a
Rapi
d7

Emer
gent

Thre
at

advis
ory

that
just

went
out

with
their

articl
e by

Caitli
n

Cond
on

toda
y.

[rapid
7.co
m/bl
og/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
is