Threat Grid Appliance version 2.12.0.1 - 2.12.2 Radius bug workaround

Contents

Introduction

On Threat Grid Appliance between version 2.12.0.1 - 2.12.2, a bug was introduced which breaks the Radius authentication support.

A permanent fix will be available in next software release.

This article will discuss the short-time workaround, which is valid until next reboot. This workaround is possible to apply if the user has access to Opadmin portal (assuming Authentication was configured to use either Radius or System Authentication)

If the user does not have access to Opadmin, please create a TAC case to troubleshoot the issue.

Problem

After upgrading to between 2.12.0.1 - 2.12.2, Radius authentication doesn’t work for both Opadmin and Clean interface portal.

Solution

In appliance 2.12.1, support is added for "signed commands" -- JSON documents which, when fed to opadmin (Support > Execute Command), run specific commands as root.

Using signed command we can implement a workaround for this bug until next reboot. [This bug is fixed in 2.12.3]

Procedure

As first step Reboot the appliance.

Then follow below instructions -

Using Opadmin Portal:

1. Login to Opadmin portal using system authentication method, browse to **Support > Execute Command**

2. Copy following command and execute it:

```
-----BEGIN PGP SIGNED MESSAGE----- X-Padding: TG-Proprietary-v1 {"command":["/usr/bin/bash","-
c","set -e\nmkdir -p -- /run/systemd/system/radialjacket.service.d\ncat
>/run/systemd/system/radialjacket.service.d/fix-execstart.conf
<<'EOF'\n[Service]\nExecStart=\nExecStart=/usr/bin/with-custom-resolver /etc/resolv.conf-
integration.d /usr/bin/without-mounts --fs-type=nfs --fs-type=nfs4 --fs-type=fuse --fs-
type=fuse.gocryptfs -- setpriv --reuid=integration --regid=integration --inh-caps=-all --clear-
groups -- /usr/bin/radialjacket -c client.crt -k client.key -r server-ca.crt -e
${host}\nEOF\nsed -i -e s@authmode@auth_mode@ /opt/appliance-
config/ansible/sandcastle.confdir.d/!pre-run/generate-face-json\ntouch
/etc/conf.d/radialjacket.conf\nset +e\n\nretval=0\nsystemctl daemon-reload || (( retval |= $?
))\nsystemctl restart config-template@sandcastle || (( retval |= $? ))\nsystemctl reload --no-
block opadmin || (( retval |= $? ))\nsystemctl restart tg-face radialjacket || (( retval |= $?
))\nexit \"$retval\""],"environment":{"PATH":"/bin:/usr/bin"},"restrictions":{"version-not-
after":"2020.04.20210209T215219","version-not-
before":"2020.04.20201023T235216.srchash.3b87775455e9.rel"}} -----BEGIN PGP SIGNATURE-----
wsBcBAABCAAQBQJgR41LCRBGH+fCiPqfvgAArtQIAHCYjCwfBtZNA+pDAnlNqI5zHt8WO38jmlCL
gWFPnYkTZH/z8JbMMsxYOrLmV+cj8sc0SKlIGUP+i8DDXh01JQCmIhGLbXtGEFqHTeizEWt7Cjxx
XjnG2BOZxR2wBtS7xTxfV5v8hA5bVTf+dd0rJHy0zgmfKI4KDvAF1i0DBuOQj+qGPo324j+Lr7uB
7UfnP2mCYpgoqzalUmseCfip+F45CXZNkUKReH4nId7wnln+51cSj++i2bVued0juSOQIib+jId7
ZlfcgWbTkN2UbTclWjArPjdemZcG5Sbsg2k/lSzkf6ni2kfu2PKe0tJjd0zMjlMqSkeSTaVOQH7e 6Sk= -----END PGP
SIGNATURE-----
```

3. **Restart `late-tmpfiles.service**` from tgsh (Console)

```
service restart late-tmpfiles.service
```

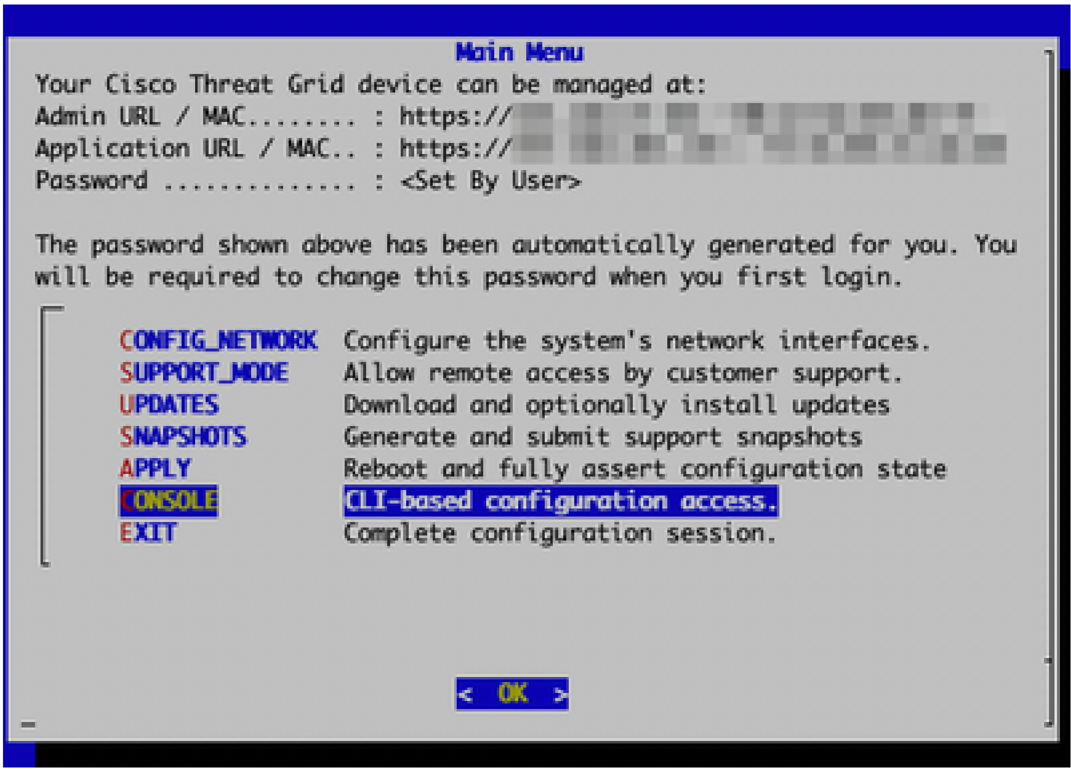
4. **Restart 'tg-face.service`** from tgsh (Console)

```
service restart tg-face.service
```

Using CONSOLE:

If the user has access to Applinace Console (TGSH), above signed command can be executed from console -

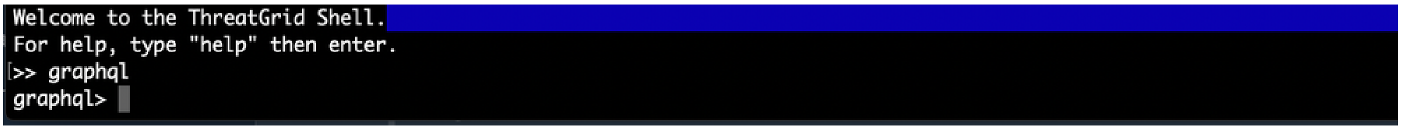
Log in to appliance console (opadmin interface), select `CONSOLE`



```
                              Main Menu
 Your Cisco Threat Grid device can be managed at:
 Admin URL / MAC........ : https://[redacted]
 Application URL / MAC.. : https://[redacted]
 Password .............. : <Set By User>

 The password shown above has been automatically generated for you. You
 will be required to change this password when you first login.

       CONFIG_NETWORK  Configure the system's network interfaces.
       SUPPORT_MODE    Allow remote access by customer support.
       UPDATES         Download and optionally install updates
       SNAPSHOTS       Generate and submit support snapshots
       APPLY           Reboot and fully assert configuration state
       CONSOLE         CLI-based configuration access.
       EXIT            Complete configuration session.

                              <  OK  >
```

Threat Grid Appliance Console

Run command `graphql` to start GraphQL interface



```
Welcome to the ThreatGrid Shell.
For help, type "help" then enter.
[>> graphql
graphql>
```

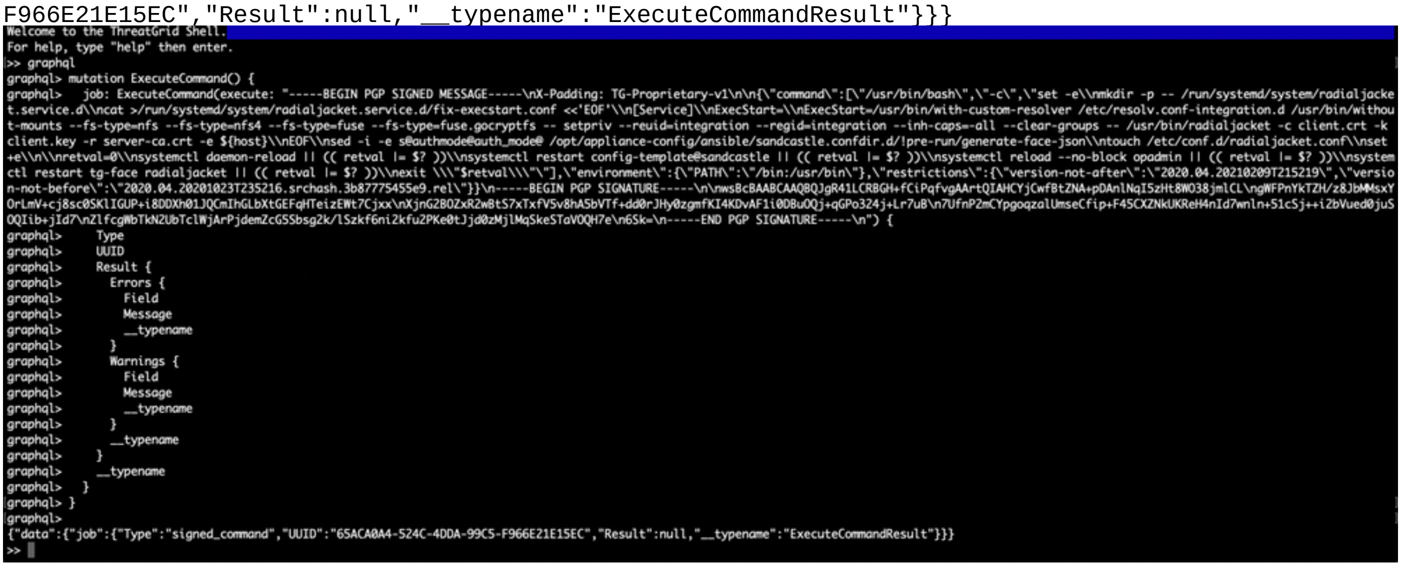
GraphQL interface

Copy following command and paste in graphql interface. Press **Enter** -

```
mutation ExecuteCommand() { job: ExecuteCommand(execute: "-----BEGIN PGP SIGNED MESSAGE-----\nX-
Padding: TG-Proprietary-v1\n\n{\"command\":[\"/usr/bin/bash\",\"-c\",\"set -e\\nmkdir -p --
/run/systemd/system/radialjacket.service.d\\ncat
>/run/systemd/system/radialjacket.service.d/fix-execstart.conf
<<'EOF'\\n[Service]\\nExecStart=\\nExecStart=/usr/bin/with-custom-resolver /etc/resolv.conf-
integration.d /usr/bin/without-mounts --fs-type=nfs --fs-type=nfs4 --fs-type=fuse --fs-
type=fuse.gocryptfs -- setpriv --reuid=integration --regid=integration --inh-caps=-all --clear-
groups -- /usr/bin/radialjacket -c client.crt -k client.key -r server-ca.crt -e
${host}\\nEOF\\nsed -i -e s@authmode@auth_mode@ /opt/appliance-
config/ansible/sandcastle.confdir.d/!pre-run/generate-face-json\\ntouch
/etc/conf.d/radialjacket.conf\\nset +e\\n\\nretval=0\\nsystemctl daemon-reload || (( retval |=
$? ))\\nsystemctl restart config-template@sandcastle || (( retval |= $? ))\\nsystemctl reload --
no-block opadmin || (( retval |= $? ))\\nsystemctl restart tg-face radialjacket || (( retval |=
$? ))\\nexit
\\\"$retval\\\"\"],\"environment\":{\"PATH\":\"/bin:/usr/bin\"},\"restrictions\":{\"version-not-
after\":\"2020.04.20210209T215219\",\"version-not-
before\":\"2020.04.20201023T235216.srchash.3b87775455e9.rel\"}}\n-----BEGIN PGP SIGNATURE-----
\n\nwsBcBAABCAAQBQJgR41LCRBGH+fCiPqfvgAArtQIAHCYjCwfBtZNA+pDAnlNqI5zHt8WO38jmlCL\ngWFPnYkTZH/z8J
bMMsxYOrLmV+cj8sc0SKlIGUP+i8DDXh01JQCmIhGLbXtGEFqHTeizEWt7Cjxx\nXjnG2BOZxR2wBtS7xTxfV5v8hA5bVTf+
dd0rJHy0zgmfKI4KDvAF1i0DBuOQj+qGPo324j+Lr7uB\n7UfnP2mCYpgoqzalUmseCfip+F45CXZNkUKReH4nId7wnln+51
cSj++i2bVued0juSOQIib+jId7\nZlfcgWbTkN2UbTclWjArPjdemZcG5Sbsg2k/lSzkf6ni2kfu2PKe0tJjd0zMjlMqSkeS
TaVOQH7e\n6Sk=\n-----END PGP SIGNATURE-----\n") { Type UUID Result { Errors { Field Message
__typename } Warnings { Field Message __typename } __typename } __typename } }
```

You will see output similar to following output, UUID will be different -

```
{"data":{"job":{"Type":"signed_command","UUID":"65ACA0A4-524C-4DDA-99C5-
F966E21E15EC","Result":null,"__typename":"ExecuteCommandResult"}}}
```



```
Welcome to the ThreatGrid Shell.
For help, type "help" then enter.
>> graphql
graphql> mutation ExecuteCommand() {
graphql>   job: ExecuteCommand(execute: "-----BEGIN PGP SIGNED MESSAGE-----\nX-Padding: TG-Proprietary-v1\n\n{\"command\":[\"/usr/bin/bash\",\"-c\",\"set -e\\nmkdir -p -- /run/systemd/system/radialjacke
t.service.d\\ncat >/run/systemd/system/radialjacket.service.d/fix-execstart.conf <<'EOF'\\n[Service]\\nExecStart=\\nExecStart=/usr/bin/with-custom-resolver /etc/resolv.conf-integration.d /usr/bin/withou
t-mounts --fs-type=nfs --fs-type=nfs4 --fs-type=fuse --fs-type=fuse.gocryptfs -- setpriv --reuid=integration --regid=integration --inh-caps=-all --clear-groups -- /usr/bin/radialjacket -c client.crt -k
client.key -r server-ca.crt -e ${host}\\nEOF\\nsed -i -e s@authmode@auth_mode@ /opt/appliance-config/ansible/sandcastle.confdir.d/!pre-run/generate-face-json\\ntouch /etc/conf.d/radialjacket.conf\\nset
+e\\n\\nretval=0\\nsystemctl daemon-reload || (( retval |= $? ))\\nsystemctl restart config-template@sandcastle || (( retval |= $? ))\\nsystemctl reload --no-block opadmin || (( retval |= $? ))\\nsystem
ctl restart tg-face radialjacket || (( retval |= $? ))\\nexit \\\"$retval\\\"\"],\"environment\":{\"PATH\":\"/bin:/usr/bin\"},\"restrictions\":{\"version-not-after\":\"2020.04.20210209T215219\",\"versio
n-not-before\":\"2020.04.20201023T235216.srchash.3b87775455e9.rel\"}}\n-----BEGIN PGP SIGNATURE-----\n\nwsBcBAABCAAQBQJgR41LCRBGH+fCiPqfvgAArtQIAHCYjCwfBtZNA+pDAnlNqI5zHt8WO38jmlCL\ngWFPnYkTZH/z8JbMMsxY
OrLmV+cj8sc0SKlIGUP+i8DDXh01JQCmIhGLbXtGEFqHTeizEWt7Cjxx\nXjnG2BOZxR2wBtS7xTxfV5v8hA5bVTf+dd0rJHy0zgmfKI4KDvAF1i0DBuOQj+qGPo324j+Lr7uB\n7UfnP2mCYpgoqzalUmseCfip+F45CXZNkUKReH4nId7wnln+51cSj++i2bVued0juS
OQIib+jId7\nZlfcgWbTkN2UbTclWjArPjdemZcG5Sbsg2k/lSzkf6ni2kfu2PKe0tJjd0zMjlMqSkeSTaVOQH7e\n6Sk=\n-----END PGP SIGNATURE-----\n") {
graphql>     Type
graphql>     UUID
graphql>     Result {
graphql>       Errors {
graphql>         Field
graphql>         Message
graphql>         __typename
graphql>       }
graphql>       Warnings {
graphql>         Field
graphql>         Message
graphql>         __typename
graphql>       }
graphql>       __typename
graphql>     }
graphql>     __typename
graphql>   }
graphql> }
graphql>
{"data":{"job":{"Type":"signed_command","UUID":"65ACA0A4-524C-4DDA-99C5-F966E21E15EC","Result":null,"__typename":"ExecuteCommandResult"}}}
>> 
```

After that **Restart `late-tmpfiles.service` and `tg-face.service` f**rom tgsh (Console)

```
service restart late-tmpfiles.service

service restart tg-face.service
```

WARNING: This will implement a workaround only until next reboot.

User can upgrade to 2.12.3 (when available) to fix this bug permanently.