Threat Grid裝置版本2.12.0.1 - 2.12.2 Radius錯誤解決方法

目錄

簡介

在2.12.0.1版到2.12.2版之間的Threat Grid裝置上，引入了一個破壞Radius身份驗證支援的錯誤。

下一個軟體版本提供永久修復。

本文將討論到下次重新啟動之前有效的短期解決方法。 如果使用者有權訪問Opadmin門戶（假設身份驗證配置為使用Radius或系統身份驗證），則可以應用此解決方法

如果使用者無法存取Opadmin，請建立TAC案例以進行疑難排解。

問題

升級到2.12.0.1 - 2.12.2之間後，Radius驗證不適用於Opadmin和Clean介面入口網站。

解決方案

在裝置2.12.1中，新增了「簽名命令」— JSON文檔的支援，這些文檔在傳送到opadmin（支援>執行命令）時，以root使用者身份運行特定命令。

使用已簽名的命令，我們可以針對此錯誤實施一個解決方法，直到下次重新啟動。[此錯誤已在2.12.3中修正]

程式

作為第一步，重新啟動裝置。

然後遵循以下說明 —

使用Opadmin門戶：

1. 使用系統身份驗證方法登入Opadmin門戶，瀏覽至**Support > Execute Command**
2. 複製以下命令並執行：

```
-----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.從tgsh重新啟動「late-tmpfiles.service」（控制檯）

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

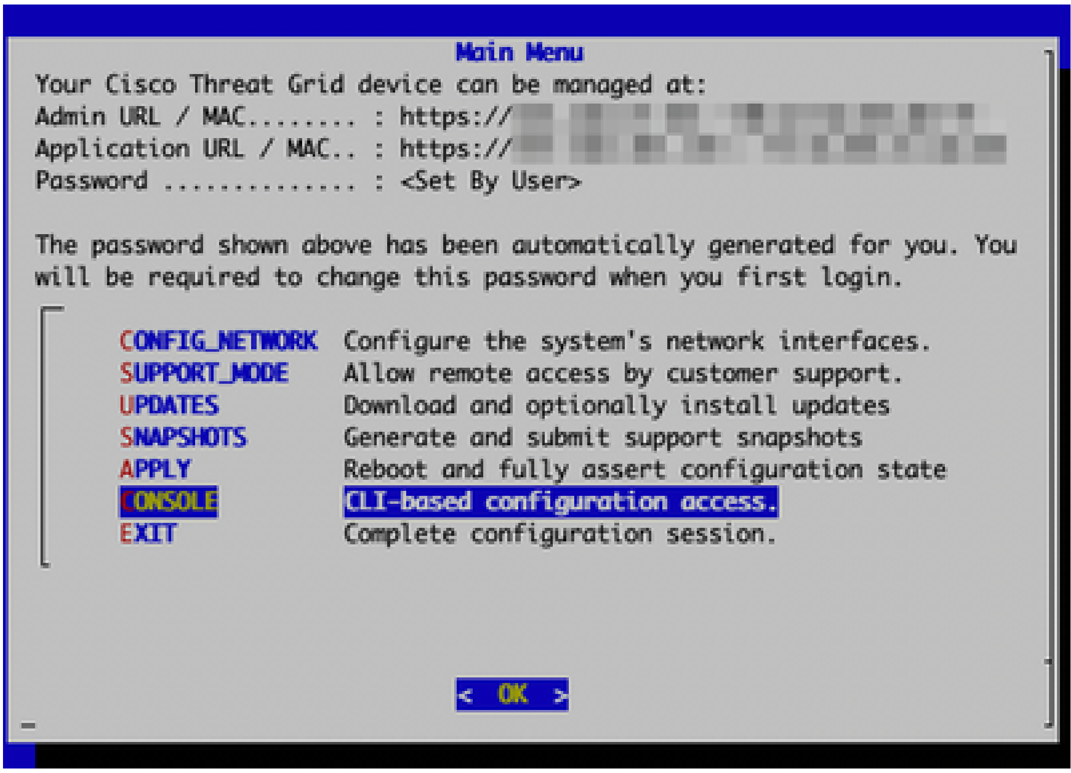
4.從tgsh（控制檯）重新啟動「tg-face.service」

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

使用控制檯：

如果使用者有權訪問Appliance Console(TGSH)，則可以從控制檯執行上面簽名的命令 —

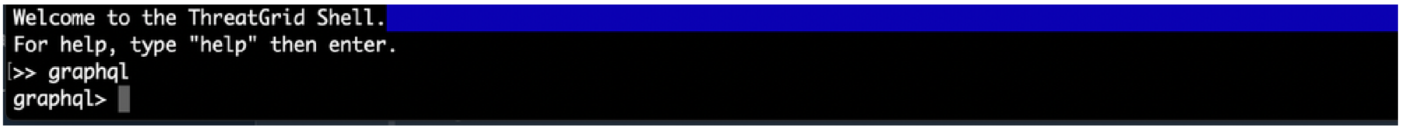
登入到裝置控制檯(opadmin interface)，選擇「CONSOLE」



```
                              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裝置控制檯

運行命令「graphql」以啟動GraphQL介面



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

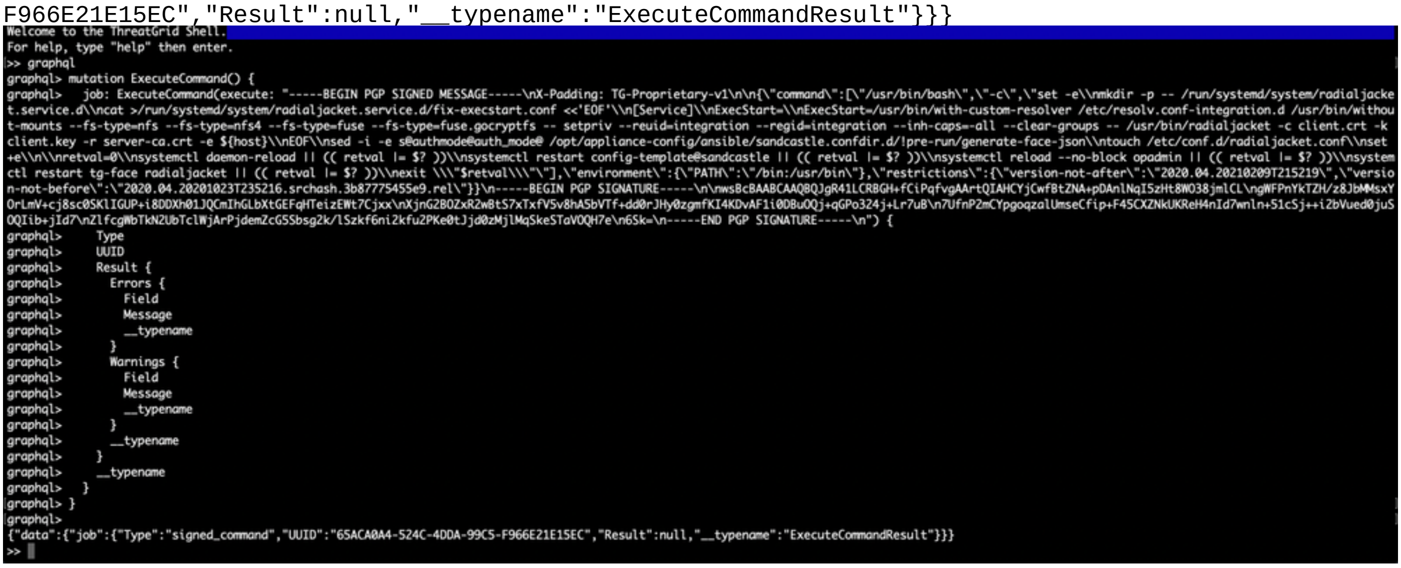
GraphQL介面

複製以下命令並貼上到graphql介面中。按**Enter**鍵 —

```
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 } }
```

您將看到類似於以下輸出的輸出，UUID將不同 —

```
{"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"}}}
>> 
```

然後**從tgsh（控制檯）重新啟動「late-tmpfiles.service」和「tg-face**.service」

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

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

警告：這僅在下次重新啟動之前實施解決方法。

使用者可以升級到2.12.3（若有），永久修正此錯誤。