Solução de problemas do Threat Grid Appliance versão 2.12.0.1 - 2.12.2 Radius

Contents

Introduction

No Threat Grid Appliance entre a versão 2.12.0.1 - 2.12.2, foi introduzido um bug que interrompe o suporte à autenticação Radius.

Uma correção permanente estará disponível na próxima versão do software.

Este artigo discutirá a solução temporária, válida até a próxima reinicialização. Esta solução alternativa é possível aplicar se o usuário tiver acesso ao portal Opadmin (supondo que a autenticação tenha sido configurada para usar o Radius ou a autenticação do sistema)

Se o usuário não tiver acesso ao Opadmin, crie um caso TAC para solucionar o problema.

Problema

Depois de atualizar para entre 2.12.0.1 e 2.12.2, a autenticação Radius não funciona para o portal de interface Opadmin e Clean.

Solução

No appliance 2.12.1, é adicionado suporte para "comandos assinados" — documentos JSON que, quando enviados para opadmin (Suporte > Executar comando), executam comandos específicos como raiz.

Usando um comando assinado, podemos implementar uma solução alternativa para este bug até a próxima reinicialização. [Este foi corrigido na versão 2.12.3]

Procedimento

Na primeira etapa, Reinicialize o dispositivo.

Siga as instruções abaixo:

Usando o portal Opadmin:

1. Faça login no portal Opadmin usando o método de autenticação do sistema, vá até **Support**

> Execute Command

2. Copie o seguinte comando e execute-o:

```
-----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. Reinicie `late-tmpfiles.service' de tgsh (Console)

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

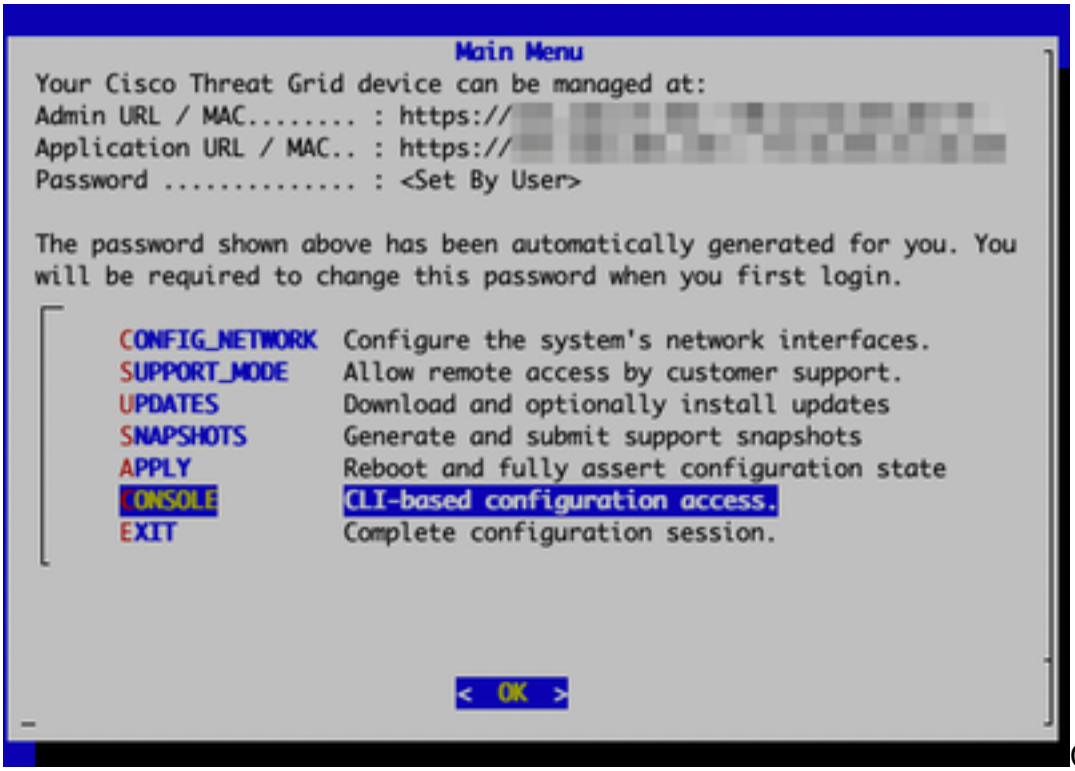
4. Reiniciar 'tg-face.service' a partir de tgsh (Console)

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

Usando CONSOLE:

Se o usuário tiver acesso ao Console do aplicativo (TGSH), o comando assinado acima poderá ser executado no console -

Faça login no console do aplicativo (interface opadmin), selecione `CONSOLE`



Console do Threat Grid Appliance

Execute o comando `grafql` para iniciar a interface GraphQL

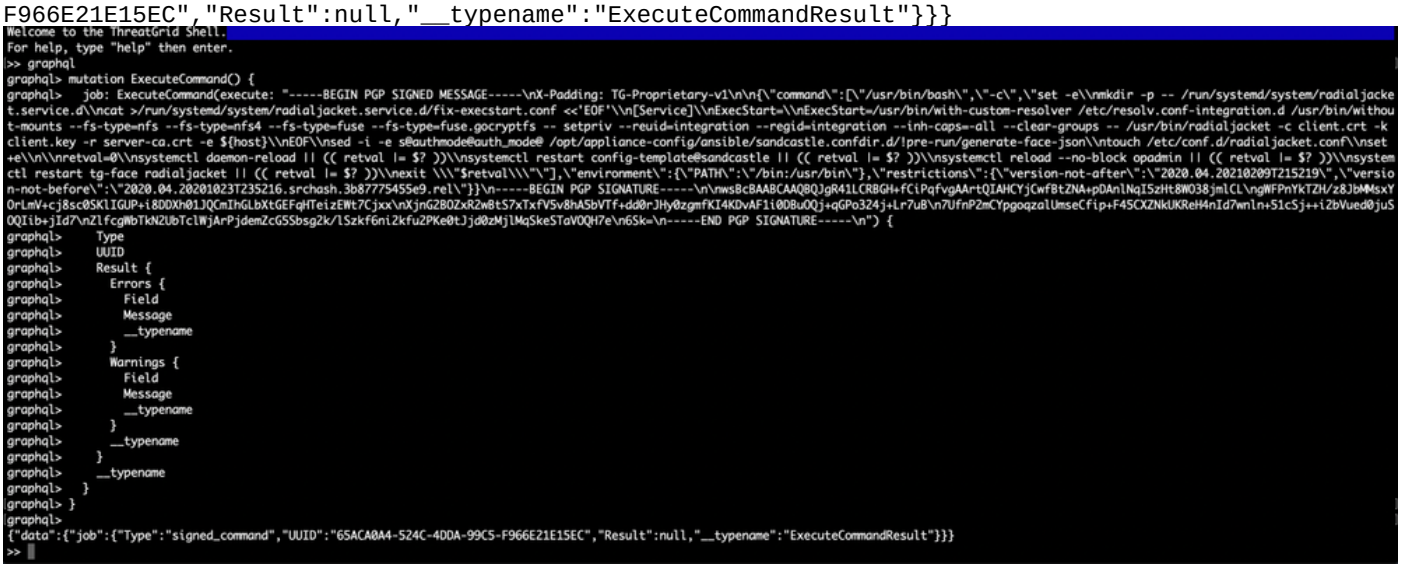
interface GraphQL

Copie o comando a seguir e cole na interface gráfica. Pressione 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 } }
```

Você verá uma saída semelhante à seguinte, UUID será diferente -

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



Depois disso, **reinicie o arquivo `late-tmpfiles.service' e o arquivo `tg-face.service'** do tgsh (Console)

```
service restart late-tmpfiles.service

service restart tg-face.service
```

AVISO: Isso implementará uma solução alternativa somente até a próxima reinicialização.

O usuário pode atualizar para 2.12.3 (quando disponível) para corrigir esse bug permanentemente.