Threat Grid设备版本2.12.0.1 - 2.12.2 Radius漏洞解决方法

目录

简介

在版本2.12.0.1 - 2.12.2之间的Threat Grid设备上，引入了一个Bug，它中断了Radius身份验证支持。

下一个软件版本中将提供永久修复。

本文将讨论短时解决方法，该方法在下次重新启动之前有效。 如果用户有权访问Opadmin门户，则可以应用此解决方法（假设Authentication配置为使用Radius或System Authentication）

如果用户无权访问Opadmin，请创建TAC案例以排除问题。

问题

升级到2.12.0.1 - 2.12.2之间后，Radius身份验证对Opadmin和Clean接口门户都不起作用。

解决方案

在设备2.12.1中，为“签名命令”（JSON文档）添加了支持，当输入到opadmin（支持>执行命令）时，JSON文档以root身份运行特定命令。

使用signed命令，我们可以对此漏洞实施解决方法，直到下次重新启动。[此Bug在2.12.3中已修复]

步骤

第一步重新启动设备。

然后按照以下说明操作 —

使用Opadmin门户：

1. 使用系统身份验证方法登录Opadmin门户，浏览到**Support > Execute Command**
2. 复制以下命令并执行：

```
-----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.从**tgsh(控制台)重新启动"late-tmpfiles.service"**

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

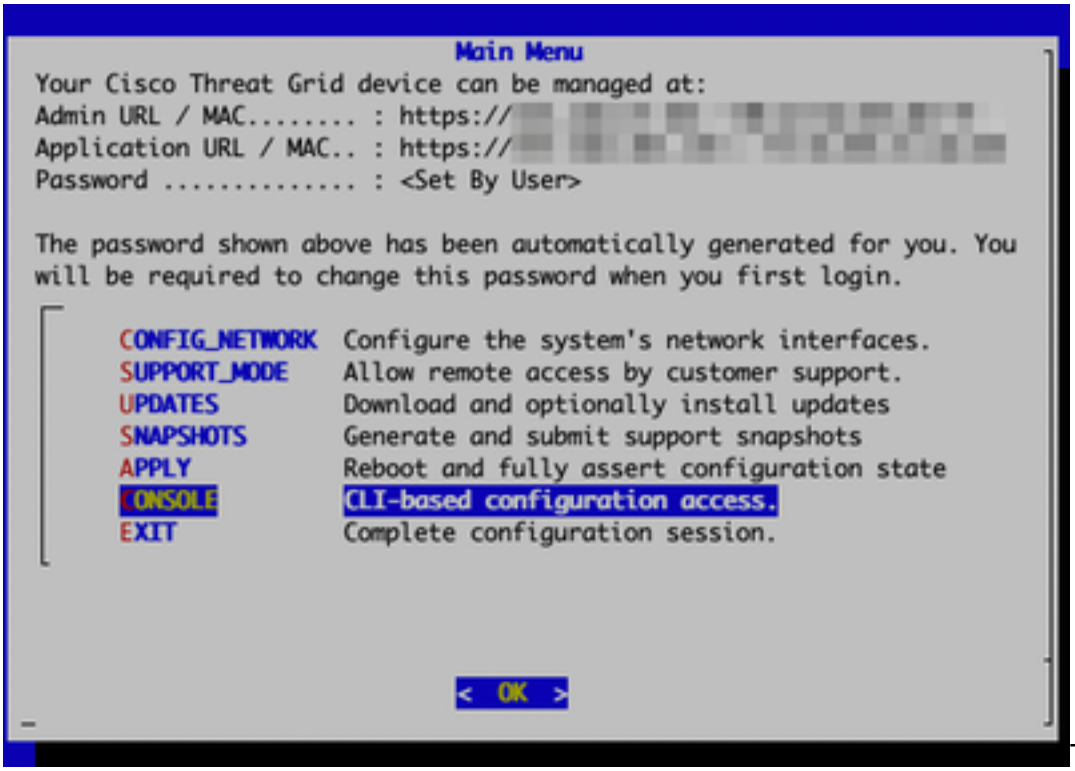
4.从**tgsh（控制台）重新启**动"tg-face.service"

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

使用控制台：

如果用户有权访问设备控制台(TGSH)，则可以从控制台执行上述签名命令 —

登录到设备控制台（opadmin接口），选择"CONSOLE"



Threat Grid设备控制台

运行命令graphql启动GraphQL接口

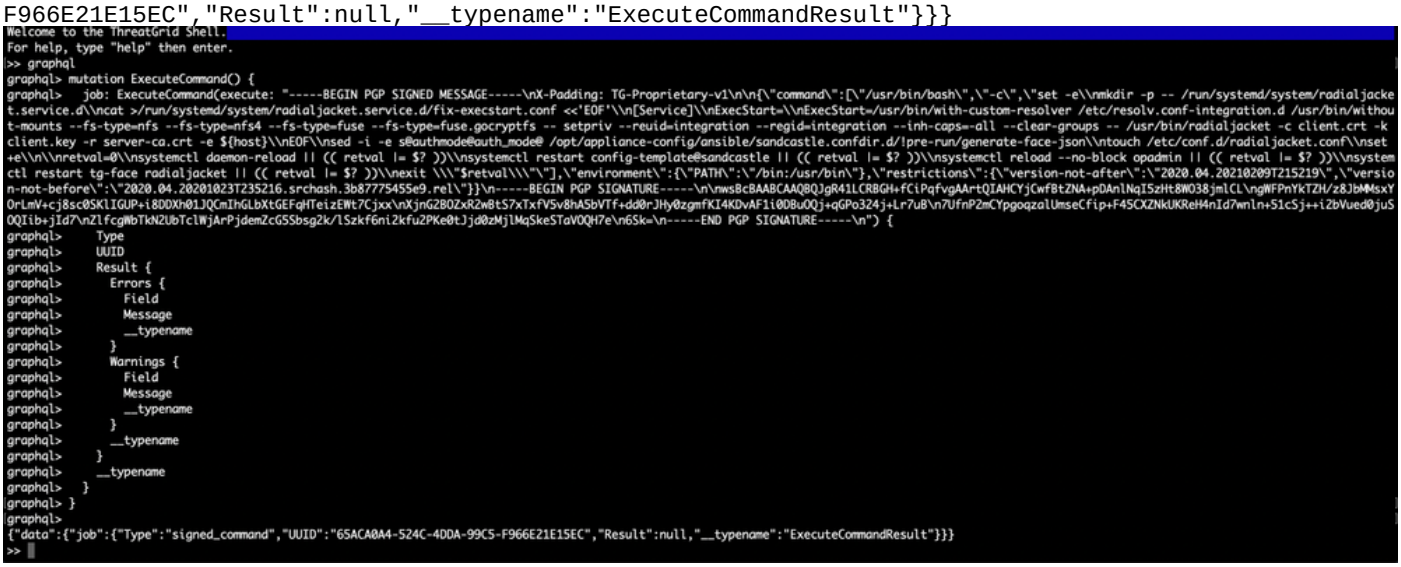
GraphQL接口

复制以下命令并粘贴到图形界面中。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 } }
```

您将看到类似以下输出的输出，UUID将不同 —

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



之后，从tgsh（控制台）重新启动“late-tmpfiles.service”和“tg-face.service”

```
service restart late-tmpfiles.service

service restart tg-face.service
```

警告：此操作将只实施一种解决方法，直到下次重新启动。

用户可以升级到2.12.3（如果可用）以永久修复此漏洞。