Threat Grid Appliance version 2.12.0.1 - 2.12.2 Résolution des bogues Radius

Contenu

Introduction

Sur Threat Grid Appliance entre la version 2.12.0.1 et la version 2.12.2, un bogue a été introduit qui brise la prise en charge de l'authentification Radius.

Une correction permanente sera disponible dans la prochaine version du logiciel.

Cet article traite de la solution de contournement à court terme, qui est valide jusqu'au prochain redémarrage. Cette solution de contournement est possible si l'utilisateur a accès au portail Opadmin (en supposant que l'authentification a été configurée pour utiliser Radius ou l'authentification système)

Si l'utilisateur n'a pas accès à Opadmin, créez un dossier TAC pour résoudre le problème.

Problème

Après la mise à niveau vers entre 2.12.0.1 et 2.12.2, l'authentification Radius ne fonctionne pas pour le portail d'interface Opadmin et Clean.

Solution

Dans l'appliance 2.12.1, la prise en charge est ajoutée pour les « commandes signées » — documents JSON qui, lorsqu'ils sont envoyés à opadmin (Support > Execute Command), exécutent des commandes spécifiques en tant que root.

En utilisant la commande signée, nous pouvons mettre en oeuvre une solution de contournement pour ce bogue jusqu'au prochain redémarrage. [Ce bogue est réparé dans 2.12.3]

Procédure

Au cours de la première étape, redémarrez l'appliance.

Suivez ensuite les instructions ci-dessous.

Utilisation du portail Opadmin :

1. Connectez-vous au portail Opadmin à l'aide de la méthode d'authentification système, accédez à **Support > Execute Command**
2. Copiez la commande suivante et exécutez-la :

```
-----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. **Redémarrez `late-tmpfiles.service`** à partir de tgsh (Console)

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

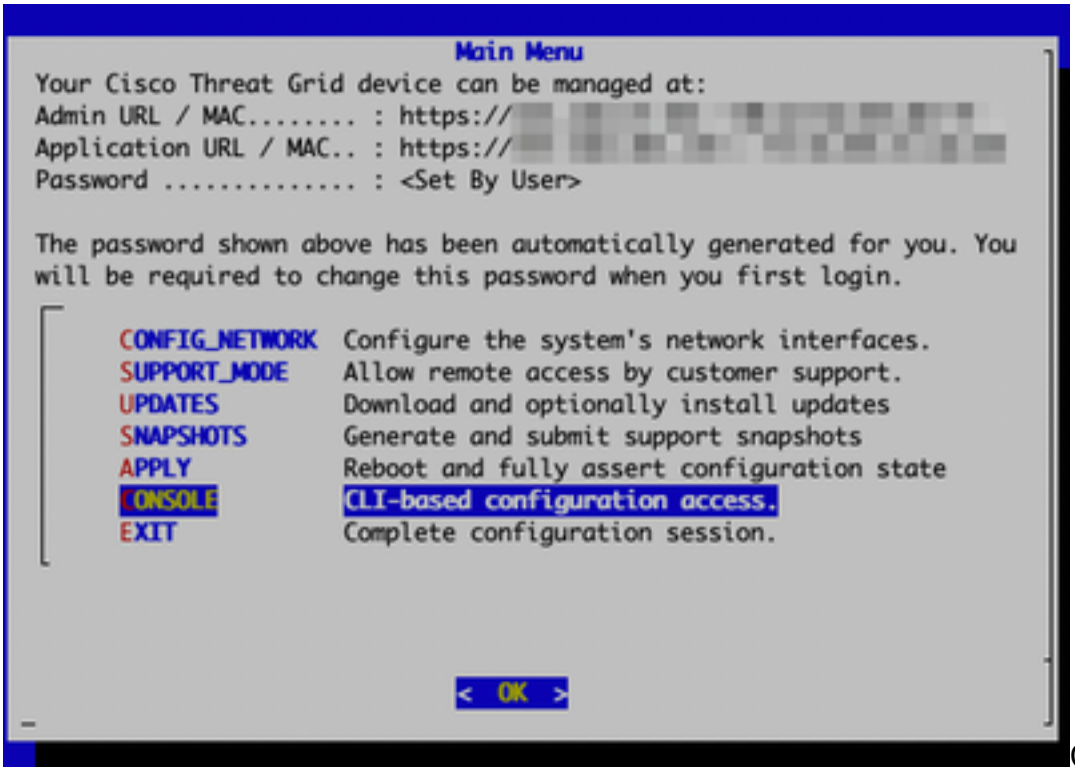
4. **Redémarrer 'tg-face.service`** à partir de tgsh (Console)

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

Utilisation de la console :

Si l'utilisateur a accès à Applinace Console (TGSH), la commande ci-dessus signée peut être exécutée à partir de la console -

Connectez-vous à la console de l'appliance (interface opadmin), sélectionnez CONSOLE



Console de l'appliance Threat Grid

Exécuter la commande `graphql` pour démarrer l'interface GraphQL

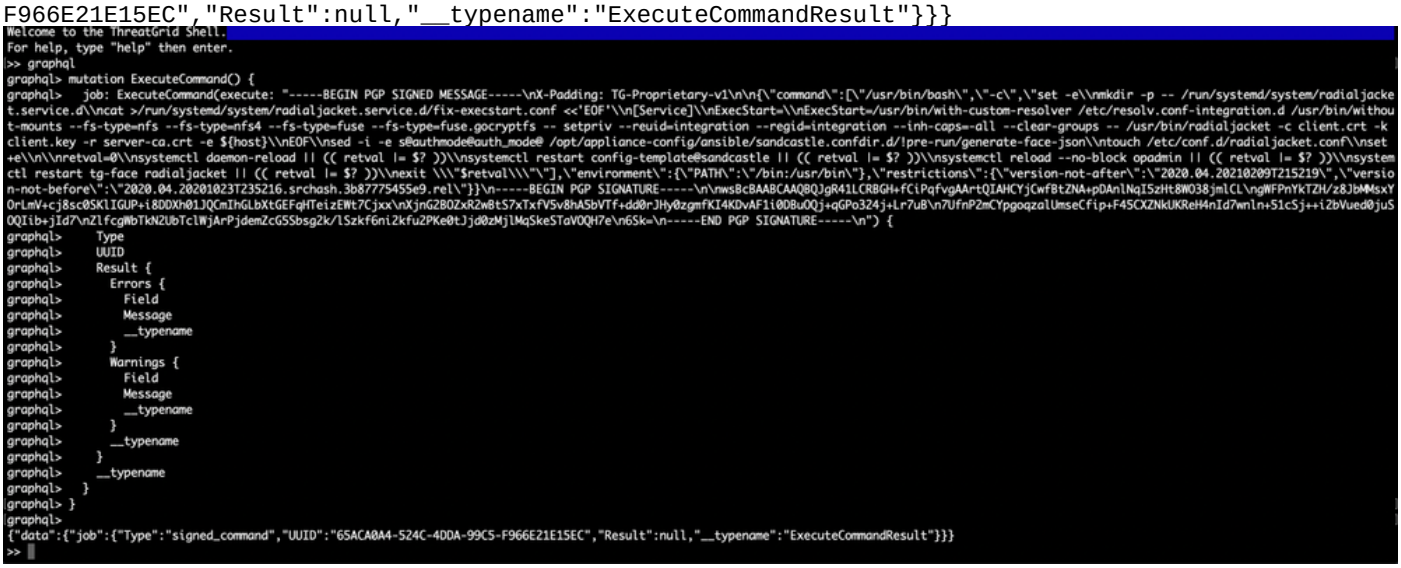
Interface GraphQL

Copiez la commande suivante et collez-la dans l'interface graphique. Appuyez sur Entrée-

```
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 } }
```

La sortie suivante s'affiche, l'UUID est différent -

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



Après cela, **redémarrez « late-tmpfiles.service » et "tg-face.service »** à partir de tgsh (Console)

```
service restart late-tmpfiles.service

service restart tg-face.service
```

AVERTISSEMENT : Cela ne mettra en oeuvre une solution de contournement que jusqu'au prochain redémarrage.

L'utilisateur peut effectuer une mise à niveau vers la version 2.12.3 (si disponible) pour corriger définitivement ce bogue.