Threat Grid Appliance Version 2.12.0.1 - 2.12.2 Radius-Bug-around

Inhalt

Einführung

Auf Threat Grid Appliance zwischen Version 2.12.0.1 und 2.12.2 wurde ein Fehler eingeführt, der die RADIUS-Authentifizierungsunterstützung unterbricht.

In der nächsten Softwareversion wird eine permanente Fehlerbehebung verfügbar sein.

In diesem Artikel wird die Kurzzeit-Problemumgehung erläutert, die bis zum nächsten Neustart gültig ist. Diese Problemumgehung kann angewendet werden, wenn der Benutzer Zugriff auf das Opadmin-Portal hat (vorausgesetzt, die Authentifizierung wurde für die Verwendung von Radius oder der Systemauthentifizierung konfiguriert).

Wenn der Benutzer keinen Zugriff auf Opadmin hat, erstellen Sie bitte ein TAC-Ticket, um das Problem zu beheben.

Problem

Nach dem Upgrade auf 2.12.0.1 - 2.12.2 funktioniert die Radius-Authentifizierung für das Opadmin- und das Clean-Interface-Portal nicht.

Lösung

In Appliance 2.12.1 wird Unterstützung für "signierte Befehle" hinzugefügt - JSON-Dokumente, die, wenn sie an opadmin (Support > Execute Command) übermittelt werden, bestimmte Befehle als root ausführen.

Mit signiertem Befehl können wir eine Lösung für diesen Fehler bis zum nächsten Neustart implementieren. [Dieser Fehler wurde in 2.12.3 behoben]

Vorgehensweise

Als ersten Schritt starten Sie die Appliance neu.

Befolgen Sie anschließend die folgenden Anweisungen:

Opadmin-Portal verwenden:

1. Melden Sie sich mithilfe der Systemauthentifizierungsmethode beim Opadmin-Portal an, und wählen Sie **Support > Execute Command aus.**
2. Kopieren Sie den folgenden Befehl und führen Sie ihn aus:

```
-----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. **Starten Sie "late-tmpfiles.service"** von tgsh (Konsole) neu.

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

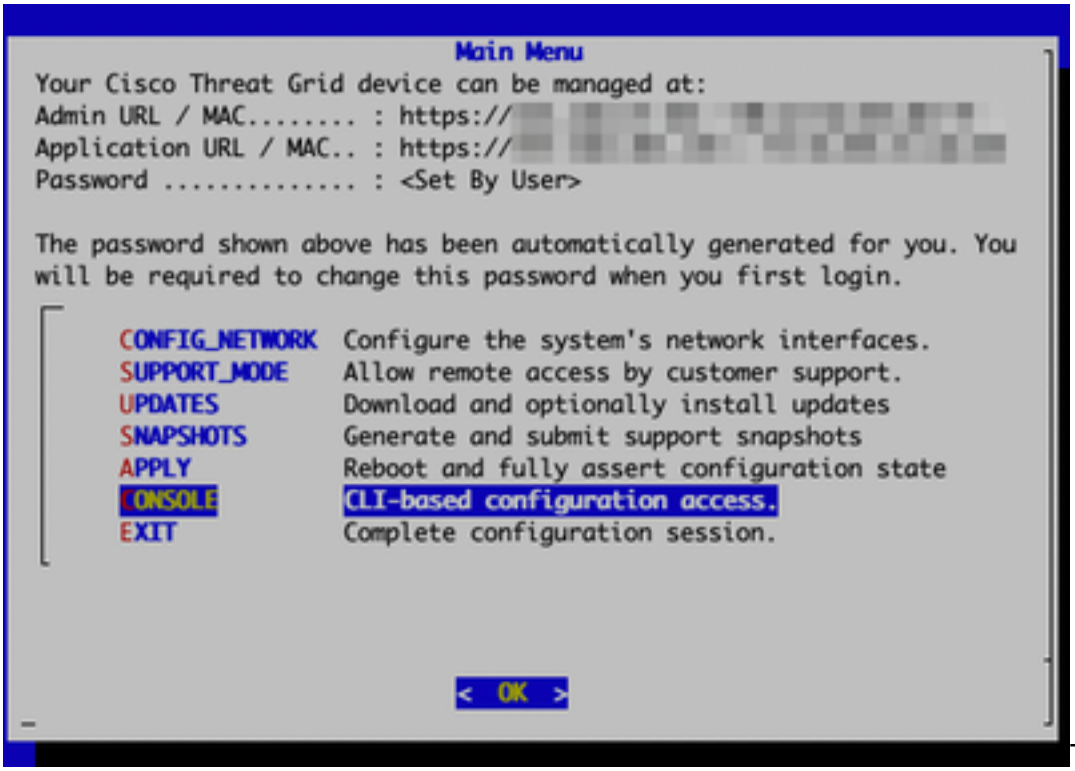
4. **Starten Sie "tg-face.service"** von tgsh (Konsole) neu.

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

Verwenden von KONSOLE:

Wenn der Benutzer Zugriff auf die Appliance Console (TGSH) hat, kann der oben signierte Befehl über die Konsole ausgeführt werden:

Melden Sie sich bei der Einheitenkonsole an (Verwaltungsoberfläche), und wählen Sie "KONSOLE" aus.



Threat Grid Appliance-Konsole

Führen Sie den Befehl `graphql` aus, um die GraphQL-Schnittstelle zu starten.

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

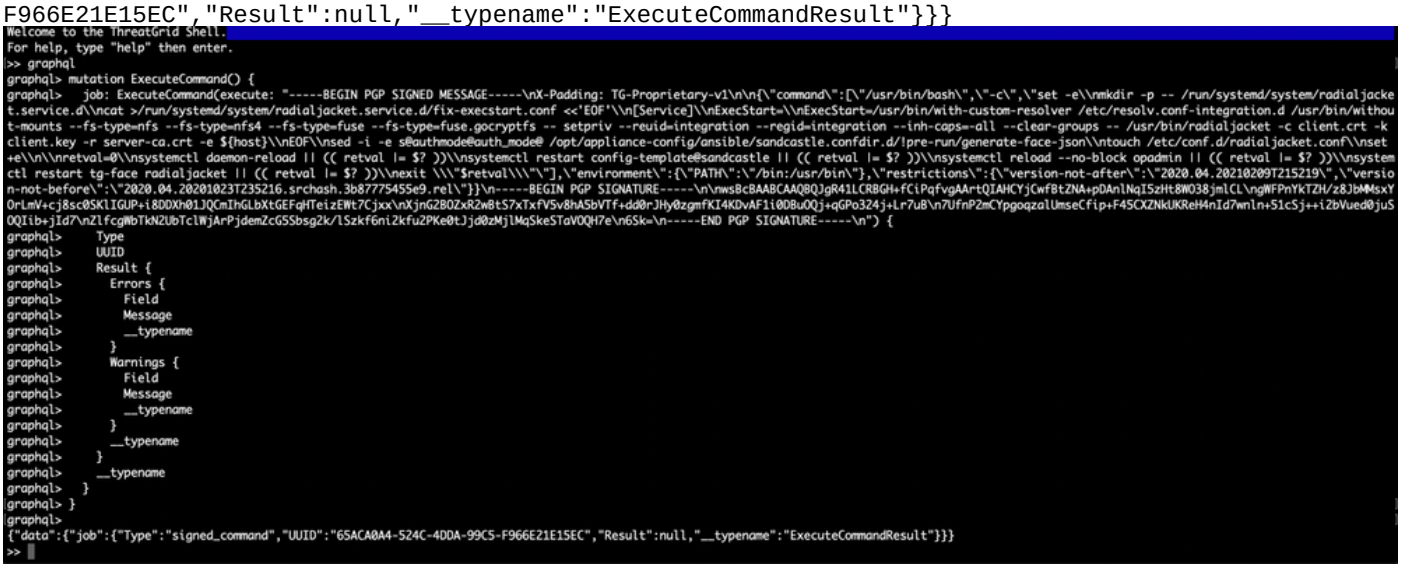
GraphQL-Schnittstelle

Kopieren Sie den folgenden Befehl und fügen Sie ihn in die grafische Oberfläche ein. Drücken Sie **die Eingabetaste** -

```
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/z8JbMMsxYOrLmV+cj8sc0SKlIGUP+i8DDXh01JQCmIhGLbXtGEFqHTeizEWt7Cjxx\nXjnG2BOZxR2wBtS7xTxfV5v8hA5bVTf+dd0rJHy0zgmfKI4KDvAF1i0DBuOQj+qGPo324j+Lr7uB\n7UfnP2mCYpgoqzalUmseCfip+F45CXZNkUKReH4nId7wnln+51cSj++i2bVued0juSOQIib+jId7\nZlfcgWbTkN2UbTclWjArPjdemZcG5Sbsg2k/lSzkf6ni2kfu2PKe0tJjd0zMjlMqSkeSTaVOQH7e\n6Sk=\n-----END PGP SIGNATURE-----\n") { Type UUID Result { Errors { Field Message __typename } Warnings { Field Message __typename } __typename } __typename } }
```

Die Ausgabe wird ähnlich der folgenden Ausgabe angezeigt. Die UUID ist anders:

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



Nach diesem **Neustart können Sie `late-tmpfiles.service` und `tg-face.service`** von tgsh (Konsole) aus starten.

```
service restart late-tmpfiles.service

service restart tg-face.service
```

WARNUNG: Dadurch wird eine Problemumgehung nur bis zum nächsten Neustart implementiert.

Benutzer können auf 2.12.3 (wenn verfügbar) aktualisieren, um diesen Fehler dauerhaft zu beheben.