Fahreddin Raşit KILIÇ | Patika-Picus Cyber Talent Academy Week 4 Task

BIG-IP iControl REST vulnerability CVE-2022-1388

Publish Date : 2022-05-05

1-) Introduction

CVE-2022-1388 affecting multiple F5 products. Requests not disclosed in this vulnerability F5 BIG-IP can bypass iControl REST authentication.

Necessary conditions of a request for exploiting this vulnerability:

1-) Connection header must include X-F5-Auth-Token

2-) X-F5-Auth-Token header must be present

3-) Host header must be localhost / 127.0.0.1 or the Connection header must include X-Forwarded-Host

4-) Auth header must be set with the admin username and any password

CVSS Score: 7.5

Confidentiality Impact: Partial (There is considerable informational disclosure.)

Integrity Impact: Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)

Availability Impact: Partial (There is reduced performance or interruptions in resource availability.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Authentication: Not required (Authentication is not required to exploit the vulnerability.)

Gained Access: None

Vulnerability Type(s): Bypass a restriction or similar

CWE ID: 306 (Missing Authentication for Critical Function)

Usage

root@kali:/home/dev# python3 CVE-2022-1388.py -t 192.168.0.221 -c id

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

2-) Impact

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.

3-) List of Products Affected by CVE-2022-1388

Big-ip Access Policy Manager (Vendor: F5)

Big-ip Advanced Firewall Manager (Vendor: F5)

Big-ip Analytics (Vendor: F5)

Big-ip Application Acceleration Manager (Vendor: F5)

Big-ip Application Security Manager (Vendor: F5)

Big-ip Domain Name System (Vendor: F5)

Big-ip Fraud Protection Service (Vendor: F5)

Big-ip Global Traffic Manager (Vendor: F5)

Big-ip Link Controller (Vendor: F5)

Big-ip Local Traffic Manager (Vendor: F5)

Big-ip Policy Enforcement Manager (Vendor: F5)

4-) Code Execution

4A-) F5 BIG-IP iControl Remote Code Execution

This Metasploit module exploits an authentication bypass vulnerability in the F5 BIG-IP iControl REST service to gain access to the admin account, which is capable of executing commands through the /mgmt/tm/util/bash endpoint. Successful exploitation results in remote code execution as the root user. Code.

4B-) F5 BIG-IP Remote Code Execution

F5 BIG-IP remote code execution proof of concept exploit that leverages the vulnerability identified in CVE-2022-1388. Code.

4C-) F5 BIG-IP 16.0.x Remote Code Execution

F5 BIG-IP version 16.0.x remote code execution exploit. Code.

5-) Recommended Actions

If you are running a version listed in the Versions known to be vulnerable column, you can eliminate this vulnerability by installing a version listed in the Fixes introduced in column. If the Fixes introduced in column does not list a version for your branch, then no update candidate currently exists for that branch and F5 recommends upgrading to a version with the fix (refer to the table). If the Fixes introduced in column lists a version prior to the one you are running, in the same branch, then your version should have the fix.

6-) Mitigation

Until it is possible to install a fixed version, you can use the following sections as temporary mitigations. These mitigations restrict access to iControl REST to only trusted networks or devices, thereby limiting the attack surface.

6A-) Block iControl REST access through the self IP address

You can block all access to the iControl REST interface of your BIG-IP system through self IP addresses. To do so, you can change the Port Lockdown setting to Allow None for each self IP address in the system. If you must open any ports, you should use the Allow Custom option, taking care to disallow access to iControl REST. By default, iControl REST listens on TCP port 443 or TCP port 8443 on single NIC BIG-IP VE instances. If you modified the default port, ensure that you disallow access to the alternate port you configured.

6B-) Block iControl REST access through the management interface

To mitigate this vulnerability for affected F5 products, you should restrict management access only to trusted users and devices over a secure network.

6C-) Modify the BIG-IP httpd configuration

In addition to blocking access through the self IP addresses and management interface, or as an alternative to blocking access if those options are not possible in your environment, you can modify the BIG-IP httpd configuration to mitigate this issue.