Severity

High

Analysis Summary

CVE-2022-1388 is a critical iControl REST authentication bypass vulnerability affecting different versions of F5 BIG-IP. F5 BIG-IP could allow a remote attacker to execute arbitrary commands on the system, caused by improper input validation. By sending specially-crafted requests to the management port and/or self IP addresses, an attacker could exploit this vulnerability to execute arbitrary commands, create or delete files, or disable services on the system.

• Snort signature for especially those organizations who did not immediately patch: alert tcp any any -> any $HTTP_PORTS (msg:”BIG-IP F5 iControl:HTTP POST URI ‘/mgmt./tm/util/bash’ and content data ‘command’ and ‘utilCmdArgs’:CVE2022-1388”; sid:1; rev:1; flow:established,to_server; flowbits:isnotset,bigip20221388.tagged; content:”POST”; http_method; content:”/mgmt/tm/util/bash”; http_uri; content:”command”; http_client_body; content:”utilCmdArgs”; http_client_body; flowbits:set,bigip20221388.tagged; tag:session,10,packets; reference:cve2022-1388; reference:url,github.com/alt3kx/CVE-2022-1388_PoC; priority:2; metadata:service http;)

Some of the verified signatures that are successful in detection of both inbound exploitation attempts (SID: 2036546) and post exploitation, indicating code execution (SID: 2036547).

- SID 2036546

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:”ET EXPLOIT F5 BIGIP iControl REST Authentication Bypass (CVE 2022-1388) M1″; flow:established,to_server; content:”POST”; http_method; content:”/mgmt/tm/util/bash”; http_uri; fast_pattern; content:”Authorization|3a 20|Basic YWRtaW46″; http_header; content:”command”; http_client_body; content:”run”; http_client_body; distance:0; content:”utilCmdArgs”; http_client_body; distance:0; http_connection; content:”x-F5-Auth-Token”; nocase; http_header_names; content:!”Referer”; content:”X-F5-Auth-Token”; flowbits:set,ET.F5AuthBypass; reference:cve,2022-1388; classtype:trojan-activity; sid:2036546; rev:2; metadata:attack_target Web_Server, created_at 2022_05_09, deployment Perimeter, deployment SSLDecrypt, former_category EXPLOIT, performance_impact Low, signature_severity Major, updated_at 2022_05_09;)

- SID 2036547

alert http $HOME_NET any -> any any (msg:”ET EXPLOIT F5 BIG-IP iControl REST Authentication Bypass Server Response (CVE 2022-1388)”; flow:established,to_client; flowbits:isset,ET.F5AuthBypass; content:”200″; http_stat_code; file_data; content:”kind”; content:”tm|3a|util|3a|bash|3a|runstate”; fast_pattern; distance:0; content:”command”; distance:0; content:”run”; distance:0; content:”utilCmdArgs”; distance:0; content:”commandResult”; distance:0; reference:cve,2022-1388; classtype:trojan-activity; sid:2036547; rev:1; metadata:attack_target Web_Server, created_at 2022_05_09, deployment Perimeter, deployment SSLDecrypt, former_category EXPLOIT, performance_impact Low, signature_severity Major, updated_at 2022_05_09;)

Affected Vendors

- F5

Affected Products

- 16.1.x versions prior to 16.1.2.2
- 15.1.x versions prior to 15.1.5.1
- 14.1.x versions prior to 14.1.4.6
- 13.1.x versions prior to 13.1.5
- All 12.1.x and 11.6.x versions

Impact

- Security Bypass
- Arbitrary System Commands
- Device Takeover

Remediation

- Quarantine potentially affected hosts
- Reimage the infected hosts
- Collect and review data, artifacts, and relevant logs.
- Upgrade F5 BIG-IP software to fixed versions (organizations using versions 12.1.x and 11.6.x should upgrade to supported versions).
- If unable to immediately patch, implement F5's temporary workarounds
- Check more information on the implementation of the workarounds here.
- Maintain and test an incident response plan.
- Prioritizes patch management and vulnerability scanning.
- Configure internet-facing network devices
- Check more considerations and guidance in case of suspecting a security compromise here