Hive Pro

THREAT ADVISORY

Have you patched this actively exploited BIG-IP vulnerability?

TA2022102

Threat Level AMBER

Publish Date – May 9, 2022

Last week, F5 patched a vulnerability tracked as CVE-2022-1388, soon after a successful Proof-of-concept(PoC) was developed by security researchers making it susceptible to further exploitation.

This authentication bypass vulnerability affects the iControl REST component in BIG-IP systems. An unauthenticated attacker could use this flaw to gain initial access and control of a vulnerable machine, allowing remote code execution.

This vulnerability has been fixed in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6 or 13.1.5. Organizations that are unable to update their versions are advised to follow these mitigations:

- Blocking iControl REST access through the self IP address
- Blocking iControl REST access through the management interface
- Modifying the BIG-IP httpd configuration

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
T1588: Obtain Capabilities
T1588.005: Obtain Capabilities: Exploits
T1588.006: Obtain Capabilities: Vulnerabilities
TA0001: Initial Access
T1190: Exploit Public-Facing Application

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-1388	F5 BIG-IP versions 16.1.x to 16.1.2.2, 15.1.x to 15.1.5.1, 14.1.x to 14.1.4.6, 13.1.x to 13.1.5, and 12.1.x and 11.6.x	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_global_traffic_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:*, cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:*	F5 BIG-IP iControl REST Authentication missing authentication vulnerability	CWE-306

Patch Link

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

References

https://twitter.com/ptswarm/status/1522873828896034816