Threat actors actively exploit F5 BIG-IP critical vulnerability CVE-2022-1388

10th May 2022

Orpheus severity score: 70

Threat actors are actively exploiting CVE-2022-1388, a critical severity vulnerability (CVSS 3: 9.8|OVSS: 45) affecting several versions of all F5 BIG-IP modules. F5 BIG-IP encompasses several appliances organisations use as load balancers, firewalls and to inspect and encrypt data entering and leaving their network.

CVE-2022-1388 appears trivial to exploit, as it requires as little as two commands and some headers sent to a vulnerable endpoint exposed to the internet. The ease with which the vulnerability can be exploited has led some security researchers to speculate its existence is due to a mistake by an F5 developer.

By exploiting CVE-2022-1388, adversaries could bypass iControl REST authentication and execute commands with root privileges, create or delete files and disable services. Forensic evidence has tracked active exploitation of the vulnerability, with adversaries dropping webshells to retain access into compromised F5 BIG-IP instances even after these have been patched.

Exploit code for CVE-2022-1388 has also become available online, mostly shared by security researchers for benign purposes. However, it is highly likely adversaries are weaponising it in their malicious campaigns. The availability of dedicated exploit code presents an opportunity to less technically savvy threat actors who would otherwise struggle to exploit CVE-2022-1388.

Given the ease with which CVE-2022-1388 can be exploited and the criticality of the system it affects, the vulnerability is poised to continue attracting attention. More than 16,000 F5 BIG-IP instances remain discoverable online, with 48 of the Fortune 50 companies actively using the system. Further, the availability of exploit code contributes to heightening the threat of exploitation. As such, we advise companies running F5 BIG-IP instances to patch

these as a matter of urgency.

Previously, we had observed both cybercriminals and state actors actively exploiting similar vulnerabilities affecting BIG-IP instances, indicating the attractiveness of the system to adversaries.

Threat Subcategory	Proof-of-Concept
Objective	Infrastructure enumeration/compromise
Target Software	F5 BIG-IP
CVE	CVE-2022-1388
Infection Vectors	Scanning/Enumeration
Source	https://www.bleepingcomputer.com/news/security/hackers-exploiting-critical-f5-big-ip-bug-public-exploits-released/ https://arstechnica.com/information-technology/2022/05/hackers-are-actively-exploiting-big-ip-vulnerability-with-a-9-8-severity-rating/