Critical Vulnerability in F5 Network Management/Security (BIG-IP) Tools

Executive Summary

The information technology vendor, F5, disclosed a significant vulnerability in their BIG-IP suite of tools which, when exploited, allows for remote code execution ultimately leading to complete compromise of the host and the potential for further compromise of the network which it sits on. These technologies are used for network/traffic management and security and are intended to support the delivery of business-critical applications. The healthcare industry is believed to operate a number of BIG-IP servers. F5 has released software updates which include fixes for this vulnerability and HC3 recommends immediate implementation of these upgrades. By updating a system, this vulnerability becomes fully patched and no longer presents an opportunity for compromise.

Report

One June 30th, the vendor F5 announced a remote code execution vulnerability in their BIG-IP Traffic Management User Interface. BIG-IP is a set of products, originally offered in 1997 as a traffic manager/load balancer which eventually evolved into an entire suite of network management and security tools. It currently includes both hardware and software-based application availability capabilities, access control functionality and a variety of different security solutions. This vulnerability is tracked as CVE-2020-5902 and has a CVSS (Common Vulnerability and Scoring System) score of 10 (critical) and it has been observed by a number of analysts and research companies as being actively exploited. The vulnerability was first reported to F5 by an independent security researcher. Just a week after initial disclosure, there are now a number of public proof of concept exploits available on social media as well as GitHub. This vulnerability is under active attack and is currently being fully exploited in in a number of organizations.

One company identified over 3,000 BIG-IP hosts vulnerable to CVE-2020-5902 fully visible from the open Internet. Another company conducted an opensource scanning/analysis of publicly-available vulnerability information and assessed that of 4,000 known, public-facing BIG-IP servers, about 50% of them were vulnerable. Vulnerable servers that are facing the public can potentially be exploited by anyone on the internet. Of these vulnerable servers, a little over one-third (736) were located in the United States. These vulnerable systems are owned by government entities, universities and other educational institutions, Fortune 500 companies, financial institutions and banks, as well as hospitals and other healthcare organizations. An independent security researcher claims to have tested about 8,000 internet-accessible BIG-IP servers and found over 5,500 vulnerable as of July 5th. It's worth noting that malicious individuals have access to the same publicly-available tools and scanners for identifying vulnerable hosts connected to the Internet.

If exploited, the attacker can potentially gain access to the Traffic Management User Interface of BIG-IP, allowing for the execution of arbitrary commands, the creation or modification of files and the ability to disable services. These conditions give an attacker virtually unlimited control over the system and not only the ability to leverage its capabilities and data for malicious purposes, but also the ability to utilize the compromised host to launch further attacks on the network. Both United States Cyber Command as well as the Department of Homeland Security both released warnings and urged organizations to patch the vulnerability.

Analyst Comment

Patches in the most recent versions of BIG-IP have been released and can be found here. They are included as part of software upgrades and HC3 recommends these upgrades be applied immediately to ensure no further possible exploitation of this vulnerability can occur. The below chart (courtesy of F5) lists the product versions and corresponding patch information. Furthermore, there are signatures available for anyone running the Snort intrusion detection system.

Product	Branch	Versions known to be vulnerable	Fixes introduced in	Severity	CVSSv3 score	Vulnerable component or feature
BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM)	15.x	15.1.0	15.1.0.4	Critical	10	TMUI/Configuration utility
		15.0.0	None			
	14.x	14.1.0 - 14.1.2	14.1.2.6			
	13.x	13.1.0 - 13.1.3	13.1.3.4			
	12.x	12.1.0 - 12.1.5	12.1.5.2			
	11.x	11.6.1 - 11.6.5	11.6.5.2			
BIG-IQ Centralized Management	7.x	None	Not applicable	Not vulnerable	None	None
	6.x	None	Not applicable			
	5.x	None	Not applicable			
Traffix SDC	5.x	None	Not applicable	Not vulnerable	None	None

References

K52145254: TMUI RCE vulnerability CVE-2020-5902
https://support.f5.com/csp/article/K52145254

CVE-2020-5902
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5902

NVD CVE-2020-5902
https://nvd.nist.gov/vuln/detail/CVE-2020-5902

F5 patches vulnerability that received a CVSS 10 severity score
https://www.zdnet.com/article/f5-patches-vulnerability-that-received-a-cvss-10-severity-score/

F5 fixes critical vulnerability discovered by Positive Technologies in BIG-IP application delivery controller
https://www.ptsecurity.com/ww-en/about/news/f5-fixes-critical-vulnerability-discovered-by-positive-technologies-in-big-ip-application-delivery-controller/

Explore BIG-IP application services
https://www.f5.com/products/big-ip-services

Over 1,800 F5 BIG-IP endpoints vulnerable to CVE-2020-5902
https://badpackets.net/over-1800-f5-big-ip-endpoints-vulnerable-to-cve-2020-5902/

Twitter (Kushagra Pathak): Just tested over ~8k BIG-IP exposed TMUI for CVE-2020-5902 and found 5527 still vulnerable! Patch now!
https://twitter.com/xKushagra/status/1279750951113539584

Twitter (US Cyber Command): URGENT: Patching CVE-2020-5902 and 5903 should not be postponed over the weekend. Remediate immediately.
https://twitter.com/CNMF_CyberAlert/status/1279151966178902016

F5 Releases Security Advisory for BIG-IP TMUI RCE vulnerability, CVE-2020-5902
https://www.us-cert.gov/ncas/current-activity/2020/07/04/f5-releases-security-advisory-big-ip-tmui-rce-vulnerability-cve

Twitter (NahamSec): CVE-2020-5902 POC
https://twitter.com/NahamSec/status/1279835507803869184

Twitter (Jin Wook Kim): F5 Big-IP CVE-2020-5902 LFI and RCE
https://twitter.com/wugeej/status/1280008779359125504

What The Heck Is F5 Networks' TMOS?
https://packetpushers.net/what-the-heck-is-f5-networks-tmos/

F5 Networks, Inc. History
http://www.fundinguniverse.com/company-histories/f5-networks-inc-history/

New Snort rule addresses critical vulnerability in F5 BIG-IP
https://blog.talosintelligence.com/2020/07/snort-rule-f5-rce-critical-vuln.html

Attackers are breaching F5 BIG-IP devices, check whether you've been hit
https://www.helpnetsecurity.com/2020/07/06/exploit-cve-2020-5902/

F5 customers urged to patch systems as critical BIG-IP flaw is actively exploited
https://portswigger.net/daily-swig/f5-customers-urged-to-patch-systems-as-critical-big-ip-flaw-is-actively-exploited

Twitter (x4ce): cve-2020-5902 proof of concept
https://twitter.com/x4ce/status/1279790599793545216

Twitter (Nep_1337_1998): CVE-2020-5902 proof of concept
https://twitter.com/Nep_1337_1998/status/1279610946864820225

Twitter (yorickkoster): CVE-2020-5902 proof of concept
https://twitter.com/yorickkoster/status/1279709009151434754

Admins Urged to Patch Critical F5 Flaw Under Active Attack
https://threatpost.com/patch-critical-f5-flaw-active-attack/157164/

Over 3,000 F5 BIG-IP endpoints vulnerable to CVE-2020-5902
https://badpackets.net/over-3000-f5-big-ip-endpoints-vulnerable-to-cve-2020-5902/

GitHub (Neo23x0): web_cve_2020_5902_f5_bigip.yml
https://github.com/Neo23x0/sigma/blob/master/rules/web/web_cve_2020_5902_f5_bigip.yml

First.org: Common Vulnerability Scoring System
https://www.first.org/cvss/