F5 fixes critical vulnerability discovered by Positive Technologies in BIG-IP application delivery controller

2 JULY 2020

Positive Technologies expert Mikhail Klyuchnikov has discovered a vulnerability in the configuration interface of the BIG-IP application delivery controller (ADC) used by some of the world's biggest companies. Attackers can run commands as an unauthorized user and completely compromise a system, including interception of controller application traffic. The vulnerability can be exploited remotely.

According to threat intelligence monitoring, Positive Technologies experts found that in June, 2020 there were more than 8,000 vulnerable devices available from the internet in the world, of which 40% lie in the United States, 16% in China, 3% in Taiwan, and 2.5% in Canada and Indonesia. Less than 1% of vulnerable devices were detected in Russia.

Vulnerability CVE-2020-5902 received a CVSS score of 10, indicating the highest degree of danger. To exploit it, an attacker needs to send a specifically crafted HTTP request to the server hosting the Traffic Management User Interface (TMUI) utility for BIG-IP configuration.

Researcher Mikhail Klyuchnikov said: *"By exploiting this vulnerability, a remote attacker with access to the BIG-IP configuration utility could, without authorization, perform remote code execution (RCE[1]). The attacker can create or delete files, disable services, intercept information, run arbitrary system commands and Java code, completely compromise the system, and pursue further targets, such as the internal network. RCE in this case results from security flaws in multiple components, such as one that allows directory traversal exploitation. This is particularly dangerous for companies whose F5 BIG-IP web interface is listed on search engines such as Shodan. Fortunately, most companies using the product do not enable access to the interface from the internet."*

Affected companies are advised to update. Vulnerable versions of BIG-IP (11.6.x, 12.1.x, 13.1.x, 14.1.x, 15.0.x, 15.1.x) should be replaced by the corresponding updated versions (11.6.5.2, 12.1.5.2, 13.1.3.4, 14.1.2.6, 15.1.0.4). Users of public cloud marketplaces such as AWS, Azure, GCP, and Alibaba should switch to BIG-IP Virtual Edition (VE) versions 11.6.5.2, 12.1.5.2, 13.1.3.4, 14.1.2.6, 15.0.1.4, or 15.1.0.4, if available. Other recommendations are given in the F5 BIG-IP bulletin. To block this and other potential attacks, companies may deploy web application firewalls such as PT Application Firewall.

F5 has provided details and recommendations in a security bulletin.

1. Remote Code Execution is one of the most critical threat according to OWASP. In 100 percent of cases, remote code execution on a server allows hacking the attacked resource.

Get in touch

Fill in the form and our specialists will contact you shortly

GENERAL QUESTIONS

We're happy to answer any questions you may have.

PARTNERSHIP

Join us in making the world a safer place.

PILOT APPLICATION

Test drive our solutions with a customized pilot program.

NAME

PHONE NUMBER

EMAIL

COUNTRY

HOW CAN WE HELP?

I give my consent to the processing of my personal data in accordance with the terms of the Privacy Notice

I give my consent to receive marketing and informational messages

SEND

market leader

Legal documents

Change region

MaxPatrol SIEM

PT AI

PT BlackBox

PT ISIM

MaxPatrol O2

MaxPatrol EDR

PT Application Firewall

PT Container Security

PT Industrial Cybersecurity Suite

ANALYTICS

Analytics articles

Knowledge base

PT ESC threat intelligence

Threatscape

Hacker groups

COMPANY

About us

Clients

Contacts

PT in the Media

Education

YouTube

Vacancy

Privacy notice

positive technologies