BACKBOX

F5 Critical TMUI RCE Vulnerability CVE-2020-5902

The Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. (CVE-2020-5902)

Description of Issue:

The above referenced vulnerability was disclosed by the vendor on July 1, 2020 and allows both authenticated and unauthenticated users to perform remote code execution (RCE).

Remote Code Execution is a type of code injection that provides an attacker the ability to run any arbitrary code on the target application, allowing them in most scenarios such as this one, to gain privileged access and perform a full system take over.

It is important to note that this vulnerability affects the administration interface only (the management dashboard) and not the underlying data plane provided by the application.

Analysis:

This vulnerability allows for unauthenticated attackers, or authenticated users, with network access to the Configuration utility, through the BIG-IP management port and/or self IPs, to execute arbitrary system commands, create or delete files, disable services, and/or execute arbitrary Java code. This vulnerability may result in a complete system compromise. The BIG-IP system in Appliance mode is also vulnerable. This issue is not exposed on the data plane; only the control plane is affected.

Important: If your BIG-IP system has TMUI exposed to the Internet and it does not have a patched version of software installed, there is a high probability that it has been compromised and you should follow your internal incident response procedures. Please see the Indications of the compromise section below.

Using BackBox Automation To Mitigate Vulnerability:

BackBox utilizes two types of automation to mitigate this vulnerability:

- BackBox IntelliChecks feature will help customers to identify which devices are exposed to the vulnerability and provide a full report on them.
- BackBox task automation will assist in upgrading the vulnerable devices to the latest version recommended by the vendor that addresses the issue that exposed this vulnerability.

Contact BackBox Today:

Please contact BackBox support at support@backbox.com

BACKBOX