Alert Bulletin

Bulletin N.: 2024-10
Publication Date: 09/05/2024
Subject: Alert 2024-10 Vulnerabilities in F5 Products
Traffic Light Protocol (TLP): White

Affected Product(s):

- **F5 BIG-IP**

Description:

A group of researchers has discovered **five vulnerabilities** in a component residing within the F5 BIG-IP product line. When exploited, these vulnerabilities grant attackers full administrative control of the device, enabling them to create accounts on any F5 asset managed by the **Next Central Manager** component. These created accounts will not be visible from the component, allowing for malicious persistence within the environment.

It is worth mentioning that there has been no active exploitation of these vulnerabilities reported worldwide. However, F5 has only acknowledged two of them, which have a severity score of **7.5**, identified as:

- **CVE-2024-21793**: OData Injection, a vulnerability that allows attackers to inject malicious data into OData queries.
- **CVE-2024-26026**: SQL Injection, which permits the execution of malicious SQL statements.

Additionally, the team that discovered the vulnerabilities insists that there are three other unacknowledged vulnerabilities that are also important, including:

- The potential for Server-Side Request Forgery (SSRF) exploitation.
- The ability to reset the admin password without authentication.
- A weakness in the hashing algorithm configuration, which may not be robust enough, creating opportunities for brute-force attacks.

Impact:

A malicious actor can exploit the vulnerabilities acknowledged by F5 to create hidden accounts, gaining persistence in F5 products and the potential for total control over the entire network of devices managed by the **Next Central Manager**.

Solution:

The vulnerabilities acknowledged by F5 have been addressed in **version 20.2.0** of the **Next Central Manager**. It is currently unknown if the unacknowledged vulnerabilities have been fixed in this patch.

Additional Information:

- Bleeping Computer Article
- Ars Technica Article
- Ars Technica Article