SecurityRisk ADVISORS

CyberSOC Threat Notification

F5 Discloses BIG-IP/BIG-IQ Vulnerabilities

Executive Summary

On March 10, 2021, F5 released a security advisory for multiple vulnerabilities, CVE-2021-22986, CVE-2021-22987, CVE-2021-22991, and CVE-2021-22992, that impact BIG-IP and BIG-IQ devices. Attackers could exploit these vulnerabilities to take control of a vulnerable system.

Description

An unauthenticated attacker could take advantage of any of these vulnerabilities to gain access to affected users. CVE-2021-22986 allows exploiters to utilize a remote command execution (RCE) vulnerability in the iControl REST interface, CVE-2021-22987 similarly is another RCE vulnerability in the Traffic Management User Interface while running in Appliance mode. CVE-2021-22991 and CVE-2021-22992 are both buffer overflow vulnerabilities, with the former occurring with an incorrectly handled request by the Traffic Management Microkernel and the latter happening when a malicious HTTP response hits an Advanced WAF/BIG-IP ASM virtual server.

Affected Products

- BIG-IP
- BIG-IP Advanced WAF/ASM
- BIG-IQ

Safeguards/Recommendations

Affected users and administrators should review the F5 advisory and install updated software as soon as possible.

Version History

Version 1. Initial Report

Vendor: F5 Networks

CVE-ID: Multiple

CVE-2021-22986,
CVE-2021-22987,
CVE-2021-22991,
CVE-2021-22992

Published: March 10, 2021

CVSS V3 Overall score: 9.8, 9.9, 9.0, 9.0

Criticality: Critical

Patch Availability: Yes

Vulnerability Type:
Remote Command Execution, Buffer Overflow

Exploitability Metrics

Attack Vector: Remote

Attack Complexity: Low, High

Privileges Required: None, Low

User Interaction: None

Impact Metrics

Scope: Changed, Changed, Unchanged, Changed

Confidentiality: High

Integrity: High

Availability: High

Confidence Metrics

Exploitability: Not Defined

Remediation Level: Not Defined

Report Confidence: Not Defined

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io