National Cyber Security Centre

21031001723-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

F5 Critical Vulnerabilities (CVE-2021-22986, CVE-2021-22987, CVE-2021-22988 & CVE-2021-20989)

2021-03-10

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Threat Type

On 10th March 2021, F5 released details of four critical CVEs with 3 further related CVEs. CSIRT-IE recommends that affected organisations review the overview from F5 here and update as soon as possible.

- **K03009991: iControl REST unauthenticated remote command execution vulnerability CVE-2021-22986:** The iControl REST interface has an unauthenticated remote command execution vulnerability. **CVSS score: 9.8 (Critical)**
- **K18132488: Appliance Mode TMUI authenticated remote command execution vulnerability CVE-2021-22987:** When running in Appliance mode, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has an authenticated remote command execution vulnerability in undisclosed pages. **CVSS score: 9.9 (Critical)**
- **K70031188: TMUI authenticated remote command execution vulnerability CVE-2021-22988:** TMUI, also referred to as the Configuration utility, has an authenticated remote command execution vulnerability in undisclosed pages. **CVSS score: 8.8 (High)**
- **K56142644: Appliance mode Advanced WAF/ASM TMUI authenticated remote command execution vulnerability CVE-2021-22989:** When running in Appliance mode with Advanced WAF or BIG-IP ASM provisioned, the TMUI, also referred to as the Configuration utility, has an authenticated remote command execution vulnerability in undisclosed pages. **CVSS score: 8.0 (High)**
- **K45056101: Advanced WAF/ASM TMUI authenticated remote command execution vulnerability CVE-2021-22990:** On systems with Advanced WAF or BIG-IP ASM provisioned, the TMUI, also referred to as the Configuration utility, has an authenticated remote command execution vulnerability in undisclosed pages. **CVSS score: 6.6 (Medium)**
- **K56715231: TMM buffer-overflow vulnerability CVE-2021-22991:** Undisclosed requests to a virtual server may be incorrectly handled by the Traffic Management Microkernel (TMM) URI normalization, which may trigger a buffer overflow, resulting in a DoS attack. In certain situations, it may theoretically allow bypass of URL based access control or remote code execution (RCE). **CVSS score: 9.0 (Critical)**
- **K52510511: Advanced WAF/ASM buffer-overflow vulnerability CVE-2021-22992:** A malicious HTTP response to an Advanced WAF/BIG-IP ASM virtual server with Login Page configured in its policy may trigger a buffer overflow, resulting in a DoS attack. In certain situations, it may allow remote code execution (RCE), leading to complete system compromise. **CVSS score: 9.0 (Critical)**

Products Affected	• Check here for a table of affected products.
Impact	Remote Code Execution
Recommendations	CSIRT-IE recommends that affected organisations install updates as a matter of urgency. All seven vulnerabilities are fixed in the following BIG-IP versions: 16.0.1.1, 15.1.2.1, 14.1.4, 13.1.3.6, 12.1.5.3, and 11.6.5.3. CVE-2021-22986 also affects BIG-IQ, and this is fixed in 8.0.0, 7.1.0.3, and 7.0.0.2.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie