National Cyber Security Centre

2205130903-NCSC

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

# NCSC Alert

## Remote Code Execution Vulnerability in iControl REST Component F5 BIG-IP (CVE-2022-1388)

## 2022-05-13

**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.*

## Description

A critical vulnerability, CVE-2022-1388, allowing remote code execution has been identified in the iControl REST component of F5 BIG-IP products. This vulnerability was announced in a security advisory by F5 and was discovered internally. The NCSC has been made aware of mass scanning for vulnerable systems and the exploitation of systems in the wild.

The vulnerability has a CVSSv3 score of 9.8.

## Products Affected

F5 BIG-IP products running:

- 16.1.0 - 16.1.2
- 15.1.0 - 15.1.5
- 14.1.0 - 14.1.4
- 13.1.0 - 13.1.4
- 12.1.0 - 12.1.6
- 11.6.1 - 11.6.5

## Impact

Potential Remote Code Execution (RCE), data theft, operations disruption, ransomware, denial of service.

## Recommendations

The NCSC recommends that affected organisations review the F5 security advisory and apply the relevant patches as soon as possible. It is also recommended that organisations conduct an investigation on all BIG-IP products that were exposed to the internet and vulnerable - F5 have an IoCs section in their advisory. Please see additional Indicators, recently released by Palo Alto.

**Mitigations:**
Users can protect themslves from external attackers by restricting access to iControl REST to only trusted networks and devices. Restrict access to the iControl REST component by following the mitigation steps in the F5 advisory.

**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