RAPID7 VULNERABILITY EXPOSURE ALERT

# F5 BIG-IP

**2021-03-19**

## Vulnerability Overview

On March 10, 2021, F5 disclosed eight vulnerabilities, four of which are deemed "critical", the most severe of which is CVE-2021-22986, an unauthenticated remote code execution weakness that enables remote attackers to execute arbitrary commands on compromised BIG-IP devices:

- K03009991: iControl REST unauthenticated remote command execution vulnerability CVE-2021-22986
- K18132488: Appliance mode TMUI authenticated remote command execution vulnerability CVE-2021-22987
- K70031188: TMUI authenticated remote command execution vulnerability CVE-2021-22988
- K56142644: Appliance mode Advanced WAF/ASM TMUI authenticated remote command execution vulnerability CVE-2021-22989
- K45056101: Advanced WAF/ASM TMUI authenticated remote command execution vulnerability CVE-2021-22990
- K56715231: TMM buffer-overflow vulnerability CVE-2021-22991
- K52510511: Advanced WAF/ASM buffer-overflow vulnerability CVE-2021-22992
- K66851119: F5 TMUI XSS vulnerability CVE-2021-22994

Rapid7 has in-depth technical analysis on this vulnerability, including proof-of-concept code and information on indicators of compromise, available on AttackerKB.

## Exploitation

On March 18, 2021, NCC Group reported in-the-wild exploitation attempts and stated that they believe final development of a complete attack chain is imminent. Other cybersecurity experts agree, prompting the creation of this VEA.

## Exposure and Patch Adoption

F5 devices are notoriously difficult to pull information from regarding versions, but is possible to identify — in some cases — whether an F5 Control Plane (i.e. management interface) is on the internet. While there are hundreds of thousands of IP addresses pointing to F5 devices on the internet, there are only (again, approximately) 4,009 exposing the Control Plane (the following table shows countries with 10 or more F5 devices exposing the Control Plane):

| Country | # F5 Exposed | % |
|---:|---:|---:|
| United States | 1,228 | 31.66% |
| China | 652 | 16.81% |
| Hong Kong SAR China | 161 | 4.15% |
| Taiwan | 146 | 3.76% |
| South Korea | 140 | 3.61% |
| Mexico | 136 | 3.51% |
| Thailand | 128 | 3.30% |
| Indonesia | 116 | 2.99% |
| Chile | 115 | 2.96% |
| Japan | 112 | 2.89% |
| Malaysia | 103 | 2.66% |
| Canada | 80 | 2.06% |
| Philippines | 74 | 1.91% |
| India | 64 | 1.65% |
| Germany | 59 | 1.52% |
| Brazil | 58 | 1.50% |
| United Kingdom | 57 | 1.47% |
| Singapore | 51 | 1.31% |
| Australia | 43 | 1.11% |
| Netherlands | 40 | 1.03% |
| Saudi Arabia | 39 | 1.01% |
| France | 38 | 0.98% |
| Peru | 33 | 0.85% |
| Ireland | 29 | 0.75% |
| South Africa | 28 | 0.72% |
| Vietnam | 25 | 0.64% |
| Spain | 22 | 0.57% |
| Turkey | 20 | 0.52% |

| | | |
|---|---|---|
| Belgium | 18 | 0.46% |
| Israel | 16 | 0.41% |
| Norway | 13 | 0.34% |
| Sweden | 13 | 0.34% |
| United Arab Emirates | 12 | 0.31% |
| Russia | 10 | 0.26% |

There are six non-telecom/carrier/cloud organizations in the Rapid7 1500 mapped industry list exposing a combined 39 F5 devices with the Control Plane exposed.

## Recommended Next Steps

Given that a complete exploit chain will be available soon, we recommend patching F5 systems that expose the affected control or data planes within the next 3–5 days and F5 systems that only expose affected planes internally within a 30-day patch window that hopefully started eight days ago, provided that your organization follows a typical 30-, 60-, 90-day prioritization scheme.

If your organization does not have a defined patch cadence system, Rapid7 still recommends that you consider applying these internal system patches within the next 20 days.

Until it is possible to install fixed versions, organizations can use the following F5 references as temporary mitigations for CVE-2021-22986 and CVE-2021-22987 to restrict access to iControl REST API endpoints:

- Block iControl REST access through the self IP address
- Block iControl REST access through the management interface

*For more information, or to obtain data specific to your organization, region, or sector, please contact research@rapid7.com.*