BIG-IP and BIG-IQ Vulnerabilities

If exploited, allows attackers to take full control over a vulnerable system

https://www.f5.com/services/support/March2021_Vulnerabilities

CVEs: CVE-2021-22986 CVE-2021-22987 CVE-2021-22991 CVE-2021-22992

The 2 most critical vulnerabilities allow a remote attacker with access to the user interface (or REST API via the user interface) to gain full control of the system and execute arbitrary system commands, create or delete files, and disable services. The most critical is unauthenticated. Exploitation can lead to complete system compromise. The U.S. Cybersecurity and Infrastructure Agency (CISA) has urged companies using BIG-IP and BIG-IQ to fix the critical F5 flaws.

Background

These are "in the wild" vulnerabilities for existing software - refer to versions listed by F5 to see if you are impacted based on the versions you may be running. Details for the 2 most critical vulnerabilities can be found in the big tables on these articles:" -

https://support.f5.com/csp/article/K18132488

-

https://support.f5.com/csp/article/K03009991

Announced

On March 10, F5 announced several vulnerabilities and strongly urged customers to upgrade: -

https://www.f5.com/services/support/March2021_Vulnerabilities

Latest Developments

On March 20, multiple stories reported the F5 vulnerabilities under "active attack". FortiGuard IPS protects against 3 of the 4 critical CVEs identified (the 4th being 22987 which requires authentication). FortiGuard Labs Threat Signal Report is available from: -

https://www.fortiguard.com/threat-signal-report/3891

Fortinet Products Summary

	Services	Version	Other Info
FortiGate	**IPS**	*18.044*	Detects CVEs 2021-22986, 2021-22991 and 2021-22992. (Not applicable to 2021-22987 which requires authentication)
FortiProxy	**IPS**	*18.044*	Detects CVEs 2021-22986, 2021-22991 and 2021-22992. (Not applicable to 2021-22987 which requires authentication)
FortiAnalyzer	**Event Handlers & Reports**	*6.2 - 7.0*	Detects IPS indicators for these F5 Big-IP and Big-IQ vulnerabilities.
FortiSIEM	**Rules & Reports**	*5.0 - 6.0*	Detects IPS indicators for these F5 Big-IP and Big-IQ vulnerabilities.

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

Exploitation

FortiGate

IPS
Version Info: 18.044
Link: https://www.fortiguard.com/updates/ips?version=18.044

FortiProxy

IPS
Version Info: 18.044
Link: https://www.fortiguard.com/updates/ips?version=18.044

Installation

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

FortiAnalyzer

Event Handlers & Reports
Version Info: 6.2 - 7.0
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD51875

FortiSIEM

Rules & Reports
Version Info: 5.0 - 6.0
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD51887