UNITED STATES SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d) of the
Securities Exchange Act of 1934

Date of Report (Date of Earliest Event Reported):
October 15, 2025

F5, Inc.

(Exact name of registrant as specified in its charter)

Washington	000-26041	91-1714307
(State or other jurisdiction of incorporation)	(Commission File Number)	(IRS Employer Identification No.)

801 5th Avenue
Seattle , WA 98104
(Address of principal executive offices) (Zip Code)

Registrant's telephone number, including area code (206) 272-5555

Not Applicable
Former name or former address, if changed since last report

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Common stock, no par value	FFIV	NASDAQ Global Select Market

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter). Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 1.05 Material Cybersecurity Incidents

On August 9, 2025, F5, Inc. (the "Company", "F5", "we", or "our") learned that a highly sophisticated nation-state threat actor had gained unauthorized access to certain Company systems. The Company promptly activated its incident response processes, and has taken extensive actions to contain the threat actor. To support these activities, the Company engaged leading external cybersecurity experts.

The Company believes its containment actions have been successful and, since the initiation of its containment efforts, has not observed any evidence of new unauthorized activity. The investigation, monitoring, and related activities are ongoing. The Company is actively engaged with federal law enforcement and government partners in connection with this incident. Additionally, the Company is implementing further measures to strengthen its security environment and protect its customers.

During the course of its investigation, the Company determined that the threat actor maintained long-term, persistent access to certain F5 systems, including the BIG-IP product development environment and engineering knowledge management platform. Through this access, certain files were exfiltrated, some of which contained certain portions of the Company's BIG-IP source code and information about undisclosed vulnerabilities that it was working on in BIG-IP. We are not aware of any undisclosed critical or remote code vulnerabilities, and we are not aware of active exploitation of any undisclosed F5 vulnerabilities. We have no evidence of modification to our software supply chain, including our source code and our build and release pipelines. This assessment has been validated through independent reviews by leading cybersecurity research firms.

We have no evidence of access to, or exfiltration of, data from our CRM, financial, support case management, or iHealth systems. However, some of the exfiltrated files from our knowledge management platform contained configuration or implementation information for a small percentage of customers. The Company is currently reviewing the contents of these files and will communicate with affected customers directly as appropriate.

We have no evidence that the threat actor accessed or modified the NGINX source code or product development environment, nor do we have evidence they accessed or modified our F5 Distributed Cloud Services or Silverline systems.

On September 12, 2025, the U.S. Department of Justice determined that a delay in public disclosure was warranted pursuant to Item 1.05(c) of Form 8-K. F5 is now filing this report in a timely manner.

As of the date of this disclosure, this incident has not had a material impact on the Company's operations, and the Company is evaluating the impact this incident may reasonably have on its financial condition or results of operations.

Item 5.02 Departure of Directors or Certain Officers; Election of Directors; Appointment of Certain Officers; Compensatory Arrangements of Certain Officers

On October 9, 2025, Michael Montoya resigned, effective immediately, from his position as a director of F5's Board of Directors (the "Board"), including his memberships on the Risk Committee and Nominating and Environmental, Social and Governance Committee. His decision to resign from the Board was not the result of any disagreement with the Company.

Mr. Montoya has been a valuable member of the Board and following his resignation from the Board, Mr. Montoya continued his service with the Company and has been appointed as F5's Chief Technology Operations Officer, effective October 13, 2025, reporting directly to the Chief Executive Officer (CEO), Montoya will lead the enterprise-wide strategy and execution to build and operate the Company with security at its core.

Pursuant to the recommendation of the Nominating and Environmental, Social and Governance Committee and in connection with Mr. Montoya's resignation, the Board reduced the size of the Board from eleven to ten members. As a result of such reduction, there are currently no vacancies on the Board.

Item 7.01 Regulation FD Disclosure

On October 15, 2025, F5 posted certain information regarding the incident on its MyF5 customer support site. A copy of that posting is furnished as Exhibit 99.1 to this report.

The information in this Item 7.01 and Exhibit 99.1 shall not be deemed to be "filed" for purposes of Section 18 of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), or otherwise subject to the liability of that section, and shall not be incorporated by reference into any registration statement or other document filed under the Securities Act of 1933, as amended, or the Exchange Act, except as shall be expressly set forth by specific reference in such filing.

Forward Looking Statements

Certain statements made in this report by F5, which are not historical facts are forward-looking statements subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. These forward-looking statements involve risks and uncertainties which we expect will or may occur in the future and may impact our business, financial condition and results of operations. The words "believe," "expect," "may," "will," "should," "could," and similar expressions are intended to identify those forward-looking statements, although there may be other such statements that do not use such wording. Such forward-looking statements include, but are not limited to, statements regarding the Company's containment efforts, the results of the Company's ongoing investigation of the incident, and the impact of the incident on the Company. These forward-looking statements reflect the Company's best judgment based on current information, and, although we base these statements on circumstances that we believe to be reasonable when made, there can be no assurance that future events will not affect the accuracy of such forward-looking information. Forward-looking statements are not guarantees of future events or circumstances and may vary materially from that discussed in this report. Factors that might cause the Company's actual results to differ materially from those anticipated in forward-looking statements include, but are not limited to: the Company's ongoing assessment of the impacts of the cybersecurity incident, including the Company's potential discovery of additional information related to the incident in connection with its investigation or otherwise; the Company's expectations regarding its ability to contain and remediate the cybersecurity incident; the impact of the cybersecurity incident on the Company's relationships with customers, employees, and governmental authorities; the legal, reputational, and financial risks resulting from the cybersecurity incident, including risks, which may arise from any potential regulatory inquiries or litigation to which the Company may become subject in connection with the incident; remediation and other additional costs that may be incurred and borne by the Company in connection with the investigation and remediation of the incident; and the risks and uncertainties discussed in the Company's annual and quarterly (including the risk factor sections) and other reports and materials provided to the

SEC. F5 disclaims any obligation to update or revise any statement contained in this report except as required by law.

Item 9.01 **Financial Statements and Exhibits**

(d) Exhibits:

Exhibit No.	Exhibit Description
99.1	Website Post dated October 15, 2025 titled "F5 Security Incident"
104.0	Cover Page Interactive Data File (embedded within the Inline XBRL document)

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

F5, INC.
(Registrant)

Date: October 15, 2025

By: */s/ François Locoh-Donou*
François Locoh-Donou
President and Chief Executive Officer

F5 Security Incident: Disclosure Statement

The following message will be posted on MyF5.com and emailed to customers

We want to share information with you about steps we've taken to resolve a security incident at F5 and our ongoing efforts to protect our customers.

In August 2025, we learned a highly sophisticated nation-state threat actor maintained long-term, persistent access to, and downloaded files from, certain F5 systems. These systems included our BIG-IP product development environment and engineering knowledge management platforms. We have taken extensive actions to contain the threat actor. Since beginning these activities, we have not seen any new unauthorized activity, and we believe our containment efforts have been successful.

In response to this incident, we are taking proactive measures to protect our customers and strengthen the security posture of our enterprise and product environments. We have engaged CrowdStrike, Mandiant, and other leading cybersecurity experts to support this work, and we are actively engaged with law enforcement and our government partners.

We have released updates for BIG-IP, F5OS, BIG-IP Next for Kubernetes, BIG-IQ, and APM clients. More information can be found in our October 2025 Quarterly Security Notification. **We strongly advise updating to these new releases as soon as possible.**

What we know
At this time, based on our investigation of available logs:

- We have confirmed that the threat actor exfiltrated files from our BIG-IP product development environment and engineering knowledge management platforms. These files contained some of our BIG-IP source code and information about undisclosed vulnerabilities we were working on in BIG-IP. We have no knowledge of undisclosed critical or remote code vulnerabilities, and we are not aware of active exploitation of any undisclosed F5 vulnerabilities.
- We have no evidence of access to, or exfiltration of, data from our CRM, financial, support case management, or iHealth systems. However, some of the exfiltrated files from our knowledge management platform contained configuration or implementation information for a small percentage of customers. We are currently reviewing these files and will be communicating with affected customers directly as appropriate.
- We have no evidence of modification to our software supply chain, including our source code and our build and release pipelines. This assessment has been validated through independent reviews by leading cybersecurity research firms NCC Group and IOActive.
- We have no evidence that the threat actor accessed or modified the NGINX source code or product development environment, nor do we have evidence they accessed or modified our F5 Distributed Cloud Services or Silverline systems.

What you can do
Our priority right now is helping you strengthen and secure your F5 environment against risks from this incident. We are providing a number of resources to support actions you can take:

- **Updates to BIG-IP software.** Updates for BIG-IP, F5OS, BIG-IP Next for Kubernetes, BIG-IQ, and APM clients are available now. Though we have no knowledge of undisclosed critical or remote code execution vulnerabilities, **we strongly advise updating your BIG-IP software as soon as possible.** More information about these updates can be found in the Quarterly Security Notification.
- **Threat intelligence.** A threat hunting guide to strengthen detection and monitoring in your environment is available from F5 support.
- **Hardening guidance with verification.** We publish best practices for hardening your F5 systems and have added automated hardening checks to the F5 iHealth Diagnostic Tool. This tool will surface gaps, prioritize actions, and provide links to remediation guidance.
- **SIEM integration and monitoring guidance.** We recommend enabling BIG-IP event streaming to your SIEM and provide step-by-step instructions for syslog configuration (KB13080) and monitoring for login

attempts (KB13426). This will enhance your visibility and alerting for admin logins, failed authentications, and privilege and configuration changes.

Our global support team is available to assist. You can open a MyF5 support case or contact F5 support directly for help updating your BIG-IP software, implementing any of these steps, or to address any questions you may have. We will keep this page updated with new information and resources.

What we are doing
We have taken, and will continue to take, significant steps to protect customers by remediating this threat and strengthening the security of our core enterprise and product infrastructure.

Since initiating our incident response efforts, we have:

- Rotated credentials and strengthened access controls across our systems.
- Deployed improved inventory and patch management automation, as well as additional tooling to better monitor, detect, and respond to threats.
- Implemented enhancements to our network security architecture.
- Hardened our product development environment, including strengthening security controls and monitoring of all software development platforms.

We are taking additional actions to further strengthen the security of our products:

- Continuing code review and penetration testing of our products with support from both NCC Group and IOActive to identify and remediate vulnerabilities in our code.
- Partnering with CrowdStrike to extend Falcon EDR sensors and Overwatch Threat Hunting to BIG-IP for additional visibility and to strengthen defenses. An early access version is available to BIG-IP customers and F5 is providing supported customers with a free Falcon EDR subscription through October 14, 2026.

Your trust matters. We know it is earned every day, especially when things go wrong. We truly regret that this incident occurred and the risk it may create for you. We are committed to learning from this incident and sharing those lessons with the broader security community.