IOActive

1426 Elliott Avenue W, Seattle, WA 98119
(866) 760.0222 | info@ioactive.com

October 10, 2025

F5, Inc.
801 5th Avenue, Seattle WA 98104

Code Review

After F5, Inc. (“F5”) was made aware of a security incident involving unauthorized access to F5’s proprietary and confidential information by a malicious actor (the “Incident”), IOActive and other advisors were engaged to assess the security threats and risks associated with its (i) covered critical F5 software source code, including critical software components of the BIG-IP product, as provided by F5, and (ii) identified portions of the software development build pipeline related to the same, and designated as critical by F5 (collectively, the “In-Scope Items”).

IOActive leveraged a suite of static analysis tools and manual code inspection looking for security flaws and back-doors that might allow privilege escalation, disclosure of sensitive information, injection of malicious code into trusted components, invalid transactions, and other conditions generally recognized as posing security vulnerabilities. This approach identifies existing attack vectors and demonstrates the potential impact of real-world attacks.

The following tasks are being performed as part of the assessment:

- Entry point analysis
- Third party dependency scanning
  - Outdated packages
  - Vulnerable packages
- Code scanning with SAST tools
- Manual code review
- Build pipeline review

IOActive is continuing to review the remaining code bases and build pipeline components as directed by F5.

In Progress Results:

IOActive did not find evidence that a threat actor introduced any vulnerabilities into the In-Scope Items.

From the source code security review, IOActive did not identify any critical severity. vulnerabilities.

Respectfully,

Roy Albert
Senior Director of Services
IOActive, Inc.

IOActive Qualifications

IOActive has more than 25 years of experience providing information security consulting services. Established in 1998, IOActive is an industry leader that specializes in:

- IT infrastructure vulnerability assessments and penetration tests
- Application security source code and architecture reviews
- ICS/SCADA and smart grid assessments and penetration tests
- Emerging market assessments and penetration tests (cloud, embedded, automotive, and more)
- Security development lifecycle training and review

IOActive works with many Global 500 companies including organizations in the power and utility, industrial, game, hardware, embedded, retail, financial, media, travel, aerospace, healthcare, high-tech, social networking, cloud, and software development industries.

We provide unequalled technical services, strive to become trusted advisors to our clients, and help them achieve their business and security objectives. We go well beyond off-the-shelf code scanning tools to perform gap analysis on information security policies and protocols. We also conduct deep analyses of information systems, software architecture, and source code using leading information risk and security management frameworks and focused threat models.

Your opponents do not use unsophisticated commercial tools to undermine your enterprise security. They use the smartest code breakers money can buy to footprint and damage your organization’s brand using advanced, often unknown methods. IOActive's industry experience helps our clients consistently stay ahead of tomorrow's threats.

IOActive attracts people who contribute to the growing body of security knowledge by speaking at elite conferences such as RSA, SANS, SOURCE, Black Hat, InfoSecurity Europe, DEF CON, Blue Hat, and CanSecWest. We also have key advisors like Steve Wozniak, luminaries who affect how security and technology shape our world.