مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – F5 Products

Tracking #:432318360

Date:06-02-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that F5 has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

F5 Networks has released its February 2026 Quarterly Security Notification (QSN), addressing multiple security vulnerabilities and exposures affecting BIG-IP, NGINX, and associated products. The vulnerabilities include medium- and low-severity CVEs, as well as security configuration exposures. Exploitation of these issues could allow unauthorized access, information disclosure, or system compromise.

Vulnerability Details:
Medium Severity CVEs:

- **CVE-2026-22548:** BIG-IP Advanced WAF or ASM security policies may trigger the bd process to terminate under certain conditions.
- **CVE-2026-1642:** NGINX OSS and NGINX Plus proxied to upstream TLS servers may allow MITM attackers to inject plain text data under specific conditions.
- **CVE-2026-22549:** BIG-IP Container Ingress Services may grant excessive permissions, allowing read access to cluster secrets.

Low Severity CVEs:

- **CVE-2026-20730:** BIG-IP Edge Client and browser VPN clients on Windows may expose sensitive information.
- **CVE-2026-20732:** An undisclosed BIG-IP configuration utility page may allow spoofed error messages.

Security Exposure:

- **BIG-IP SMTP Configuration (K000156643):** Authenticated users with guest role may modify SMTP server settings and run the Test Connection feature.

Note:
For the full list affected products, fixed versions, and detailed guidance, refer to the F5 K000159076: Quarterly Security Notification.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by F5.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://my.f5.com/manage/s/article/K000159076