



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates- Multiple Vulnerabilities in F5 Products

Tracking #:432315629

Date:20-02-2024

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 INTELLIGENCE 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 F5 recently released security updates to patch multiple vulnerabilities in its products.

TECHNICAL DETAILS:

On February 14, 2024, F5 released its Quarterly Security Notification, which addressed several vulnerabilities and security exposures affecting various F5 products. Threat actors could potentially exploit some of these vulnerabilities to take control of affected systems.

High-Severity Vulnerabilities Details:

| Article (CVE) | CVSS score | Affected products | Affected versions | Fixed Versions |
|---|------------|---|--|-----------------------------|
| K000137522: BIG-IP iControl REST vulnerability CVE-2024-22093 | 8.7 | BIG-IP (all modules) | 17.1.0 16.1.0 - 16.1.3 15.1.0 - 15.1.8 | 17.1.1 16.1.4 15.1.9 |
| K000134516: BIG-IP SSL Client Certificate LDAP and CRLDP Authentication profiles vulnerability CVE-2024-23979 | 7.5 | BIG-IP (all modules) | 17.1.0 16.1.0 - 16.1.3 15.1.0 - 15.1.8 | 17.1.1 16.1.4 15.1.9 |
| K000135873: BIG-IP Websockets vulnerability CVE-2024-21849 | 7.5 | BIG-IP (Advanced WAF/ASM) | 16.1.0 - 16.1.3 | 17.1.0 16.1.4 |
| K000135946: BIG-IP PEM vulnerability CVE-2024-23982 | 7.5 | BIG-IP (PEM) | 17.1.0 - 17.1.1 16.1.0 - 16.1.4 15.1.0 - 15.1.10 | None |
| K000137270: BIG-IP Advanced WAF and BIG-IP ASM and vulnerability CVE-2024-21789 | 7.5 | BIG-IP (Advanced WAF/ASM) | 17.1.0 | 17.1.1 |
| K000137333: BIG-IP TMM vulnerability CVE-2024-24775 | 7.5 | BIG-IP (all modules) | 17.1.0 16.1.0 - 16.1.3 15.1.0 - 15.1.9 | 17.1.1 16.1.4 15.1.10 |
| K000137334: F5 Application Visibility and Reporting module and BIG-IP Advanced WAF/ASM vulnerability CVE-2024-23805 | 7.5 | Application Visibility and Reporting module and BIG-IP (Advanced WAF/ASM) | 17.1.0 16.1.0 - 16.1.3 15.1.0 - 15.1.9 | 17.1.1 16.1.4 15.1.10 |
| K000137416: BIG-IP Advanced WAF and BIG-IP ASM vulnerability CVE-2024-23308 | 7.5 | BIG-IP (Advanced WAF/ASM) | 17.1.0 | 17.1.1 |



| | | | | |
|--|-----|----------------------|--|-----------------------------|
| K000137521: BIG-IP AFM vulnerability CVE-2024-21763 | 7.5 | BIG-IP (AFM) | 17.1.0 16.1.0 - 16.1.3 15.1.0 - 15.1.9 | 17.1.1 16.1.4 15.1.10 |
| K000137595: BIG-IP AFM signature matching vulnerability CVE-2024-21771 | 7.5 | BIG-IP (AFM + IPS) | 17.1.0 16.1.0 - 16.1.3 15.1.0 - 15.1.8 | 17.1.1 16.1.4 15.1.9 |
| K000137675: BIG-IP HTTP/2 vulnerability CVE-2024-23314 | 7.5 | BIG-IP (all modules) | 17.1.0 16.1.0 - 16.1.3 15.1.0 - 15.1.8 | 17.1.1 16.1.4 15.1.9 |
| | | BIG-IP Next SPK | 1.5.0 - 1.8.0 | 1.8.1 |
| K000138444: NGINX HTTP/3 QUIC vulnerability CVE-2024-24989 | 7.5 | NGINX Plus | R31 | R31 P1 |
| | | NGINX Open Source | 1.25.3 | 1.25.4 |
| K000138445: NGINX HTTP/3 QUIC vulnerability CVE-2024-24990 | 7.5 | NGINX Plus | R30 - R31 | R31 P1 R30 P2 |
| | | NGINX Open Source | 1.25.0 - 1.25.3 | 1.25.4 |
| K32544615: BIG-IP iControl REST API vulnerability CVE-2024-22389 | 7.2 | BIG-IP (all modules) | 17.1.0 16.1.0 - 16.1.3 15.1.0 - 15.1.8 | 17.1.1 16.1.4 15.1.9 |

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:

1. <https://my.f5.com/manage/s/article/K000138353#exposure>