Six Critical F5 Big-IP Flaws Could Lead to RCE (CVE-2026-123637, CVE-2026-121805, CVE-2026-120292, CVE-2026-120285, CVE-2026-116953, CVE-2026-120722)

Nov 19, 2026

WHITE

View Alert

On November 18, 2026, F5 disclosed six critical BIG-IP vulnerabilities that can crash the **Traffic Management Microkernel (TMM)** without authentication.

No exploitation has been reported, and F5 has provided only engineering hotfixes, with no workarounds or scheduled release fixes yet.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their risk exposure to the vulnerabilities.

Additional Info

Analysis:

On **November 18, 2026**, **F5** published advisories addressing six critical stack-based buffer overflow vulnerabilities in BIG-IP (scored **9.8** on CVSS v3.1 and **9.3** on CVSS v4.0), alongside six lower-rated flaws. These six primary issues reside in the data plane and affect specific virtual server

configurations using certain iRule commands or an **Access Policy Manager (APM)** per-request policy with Client Information and Endpoint Security agents.

While no exploitation has been observed, unauthenticated attackers could disrupt the **Traffic Management Microkernel (TMM)** or potentially execute remote code.

In the health sector, BIG-IP appliances commonly manage network traffic, load balancing, and secure remote access for electronic health record (EHR) portals and telehealth platforms. Healthcare organizations that utilize custom iRules for application routing or rely on APM endpoint security checks for clinical staff access face potential exposure. Because these flaws affect the data plane rather than the management interface, standard network segmentation of administrative ports will not prevent traffic disruption on exposed virtual servers.

Operational continuity is particularly important in clinical environments where temporary TMM restarts can interrupt real-time patient data access and connected medical workflows. Currently, F5 has not provided workarounds or scheduled release fixes for the six primary issues, offering only engineering hotfixes that undergo less extensive quality assurance testing. Health IT security teams must weigh the operational risks of deploying interim hotfixes against potential impacts on availability and integrity of patient-facing infrastructure.

Recommendations:

Health-ISAC recommends organizations review and assess their risk exposure to these vulnerabilities and implement the following:

- **Audit virtual server configurations:** Review all BIG-IP, BIG-IP Next for Kubernetes, and BIG-IP CNF deployments for the specific iRule commands *(PEM::subscriber, MR::message route, PSC::ip_address, GENERICMESSAGE::route, DNS::scrape)* and APM per-request policies listed in F5's security notification.
- **Evaluate and test engineering hotfixes:** For affected clinical or patient-facing systems, request the appropriate engineering hotfixes from F5 support and validate them in a staging environment before production deployment, noting F5's hotfix policy.
- **Apply scheduled updates for secondary flaws:** Upgrade to fixed versions *(such as BIG-IP 21.1.0.3, 17.5.1.10, or 17.1.3.6)* to remediate the six lower-rated flaws, including the iControl SOAP and REST issues.

- **Implement interim mitigations where applicable:** Restrict iControl SOAP access to trusted networks, configure scripts to delete unused iControl REST tokens, and ensure high-availability failover configurations are functioning properly to minimize service interruptions.
- **Review the Health Industry Cybersecurity Practices (HICP):** Managing Threats and Protecting Patients Resources.

<hr size=1 width="100%" align=center>

Alert Id	bb0d1ed8
Category	Vulnerability Bulletins
References	hhs thehackernews f5
Tags	CVE-2026-121805, CVE-2026-120722, CVE-2026-116953, CVE-2026-120285, CVE-2026-120292, CVE-2026-123637, Traffic Management Microkernel (TMM), F5 BIG-IP, Remote Code Execution

---

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Please provide your feedback

Like Dislike

Download the App
Available on iOS, Android and Web



For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**
Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--
You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.
To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.
To view this discussion visit https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/010001a1f28a8f7f-c95f2467-19df-4058-ae40-aa4b8a352673-000000%40email.amazonses.com.