

F5 Releases Out-of-band Security Updates for NGINX Flaws (CVE-2026-15176, CVE-2026-93479, CVE-2026-97205, and more)

Oct 19, 2026

☐ WHITE

[View Alert](#)

On October 14, 2026, F5 published an out-of-band security advisory that indexes multiple vulnerabilities affecting NGINX products and components.

Of the 11 vulnerabilities, 3 are critical ([CVE-2026-15176](#), [CVE-2026-93479](#), and [CVE-2026-97205](#)), all with a CVSS score of **9.2**. They involve heap buffer overflows in NGINX core HTTP modules and map directive configurations, potentially allowing remote denial-of-service or code execution. The remaining 8 issues hold high or medium severity ratings

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

Additional Info

Analysis:

F5's [October 14, 2026 out-of-band advisory](#) addresses 11 security vulnerabilities across NGINX components, led by 3 prominent vulnerabilities rated **9.2** on the CVSS scale, tracked as [CVE-2026-15176](#), [CVE-2026-93479](#), and [CVE-2026-97205](#). These vulnerabilities stem from memory mismanagement in the core HTTP module and configuration handling in map directives. Remote

attackers could send targeted requests that trigger worker process crashes or potentially run unauthorized code on affected deployments. The remaining nine issues pose moderate to high risks across API gateways, ingress controllers, and scripting extensions.

Below is the list of vulnerabilities included in the **October 14, 2026 Out-of-Band Advisory**:

- [CVE-2026-15176](#) (CVSS: 9.2 / Critical) - Heap buffer overflow in the NGINX core HTTP module (ngx_http_core_module) involving alias and request filename processing, potentially causing denial-of-service or remote code execution.
- [CVE-2026-97205](#) (CVSS 9.2 / Critical) - Use-after-free vulnerability in the NGINX core HTTP module (ngx_http_core_module) when AIO and Server Side Includes (include virtual) are used, which can crash worker processes or allow code execution.
- [CVE-2026-93479](#) (CVSS: 9.2 / Critical) - Heap buffer overflow in NGINX configuration handling when the map directive uses regular expression matching and references regex capture variables.
- [CVE-2026-94197](#) (CVSS: 8.7 / High) - Authentication and authorization bypass vulnerability in the NGINX Kubernetes Ingress Controller when configured with ExternalAuth policies.
- [CVE-2026-91184](#) (CVSS: 8.7 / High) - Information disclosure/rendering vulnerability in NGINX Gateway Fabric when rendering the spec.basic.realm and spec.jwt.realm fields of a namespaced authentication filter.
- [CVE-2026-104939](#) (CVSS: 8.7 / High) - Vulnerability in the NGINX Ingress Controller when implementing externalAuth policies, where mishandled OAuth IDP HTTP responses can grant unauthenticated access to protected paths.
- [CVE-2026-101019](#) (CVSS: 8.3 / High) - Interpretation conflict vulnerability in the NGINX JavaScript (njs) XML module where entity-backed XML attributes are handled inconsistently with canonicalization rules.
- [CVE-2026-97629](#) (CVSS: 8.1 / High) - Session forgery vulnerability in the NGINX SSL module (ngx_http_ssl_module) when ssl_session_cache is configured without explicit session ticket key rotation files, enabling client certificate verification bypass.
- [CVE-2026-95101](#) (CVSS: 8.1 / High) - Request-processing vulnerability in the NGINX HTTP/3 module (ngx_http_v3_module).
- [CVE-2026-101025](#) (CVSS: 6.9 (Medium) - Memory leak vulnerability in the NGINX JavaScript (njs) engine when xml.parse() fails and leaks a libxml2 parser context.
- [CVE-2026-96615](#) (CVSS: 6.5 / Medium) - Authentication bypass/exposure vulnerability in NGINX Gateway Fabric related to Gateway CRD configurations and gRPC connections with

the NGINX Agent, potentially allowing unauthorized reading of TLS private keys across namespaces.

In health sector environments, NGINX servers often serve as reverse proxies and API gateways that protect electronic health record systems, patient portals, and medical IoT devices. Process crashes can directly disrupt real-time access to clinical data and diagnostic tools. Furthermore, if threat actors achieve remote code execution, they could bypass network perimeters and access protected health information without authorization. Given the continuous operational requirements of healthcare infrastructure, even temporary system unresponsiveness poses operational and regulatory compliance risks.

Recommendations:

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

- Update affected NGINX Open Source, NGINX Plus, and ingress controller software to fixed versions immediately.
- Apply temporary configuration mitigations, such as avoiding unnamed regex captures in map directives, if patching must be delayed.
- Restrict exposure of NGINX management interfaces and data plane endpoints behind internal networks or firewalls.
- Enforce zero-trust segmentation between web proxy tiers and core electronic health record databases to limit lateral movement.
- Monitor system logs for unexpected NGINX worker process restarts or irregular incoming HTTP payloads.
- **Review the Health Industry Cybersecurity Practices (HICP): [Managing Threats and Protecting Patients](#)** Resources.

Alert Id

e4d10df0

Category

Vulnerability Bulletins

References

[f5](#) [hhs](#) [f5 1](#) [f5 2](#) [f5 3](#) [f5 4](#) [f5 5](#) [f5 6](#) [f5 7](#) [f5 8](#) [f5 9](#) [f5 10](#) [f5 11](#)

Tags

CVE-2026-97205, CVE-2026-93479, CVE-2026-15176, F5
NGINX, Regex

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/010001a152980fd6-0a446856-12ab-486c-8a7a-bcc208ede517-000000%40email.amazonses.com>.