Customer FAQ: Response to NGINX Security Vulnerabilities (NGINX2Root / CVE-2026-123007, CVE-2026-123633, CVE-2026-123634, CVE-2026-121810 & CVE-2026-113425)

1. Applicability & Exposure

Q: Do any of your products, customer-facing applications, or supporting services utilize NGINX?

Answer: Yes. NGINX is used in certain platforms, customer-facing portals, and supporting services. Following the public disclosure of the five NGINX2Root vulnerabilities on November 18, 2026, our Security team initiated discovery scans across our managed environments to identify systems running affected NGINX versions (NGINX Open Source up to 1.31.8, and affected NGINX Plus releases).

Q: Were any externally facing endpoints or services affected by these vulnerabilities?

Answer: Yes. Our assessment identified systems running affected NGINX versions, including internet-facing services. Our engineering teams are assessing the impact and applying fixes, with priority given to internet-exposed services.

November 28 2026 14:13 UTC

---

2. Immediate Mitigations & Compensating Controls

Q: What immediate actions were taken to secure externally facing endpoints prior to or alongside patching?

Answer: For identified internet-facing instances, we have applied mitigations where feasible, as appropriate to each system, to reduce exposure while updated NGINX releases are deployed. Internet-facing services are being addressed first.

---

3. Remediation & Patching Status

Q: What is the current patching status across affected systems?

Answer:

- **Externally Facing Production Endpoints:** Remediation is in progress and is our highest priority. Affected systems are being updated to vendor-patched NGINX releases, with mitigations applied where feasible in the interim.
- **Internal & Supporting Infrastructure:** Remediation of internal and non-public instances will follow, prioritized based on risk.
- **Continuous Discovery:** We use automated scanning across our managed cloud environments to help detect, isolate, and remediate newly provisioned or previously unclassified workloads.

©2026 Sinch

4. Incident Review & Impact Assessment

Q: Have you observed any evidence of active exploitation, compromise, or data breach?

Answer: Our Security Operations Center (SOC) and engineering teams are assessing the impact of these vulnerabilities on affected systems, including review of available access logs, perimeter telemetry, and host runtime data. To date, we have not identified any indicators of compromise. This assessment is ongoing, and we will update this information if our findings change.

Q: Will you notify us if exploitation or impact is identified?

Answer: If we determine that a security incident has affected your services or customer data, we will notify you in accordance with our applicable agreements, including any Data Processing Agreement, and applicable laws.

---

5. Supply Chain & Follow-Up

Q: Are you assessing third-party suppliers and sub-processors for these vulnerabilities?

Answer: Yes. Our vendor risk management team is assessing relevant vendors and third-party infrastructure providers regarding their exposure to these CVEs and their remediation plans, consistent with our vendor management program.

Q: Who is the contact for formal security follow-ups and vendor questionnaires?

Answer:
For audit inquiries, vendor questionnaires, or follow-up technical questions, please contact your account manager or our security team at security@sinch.com. Responses are provided subject to the confidentiality terms of your agreement with us.

November 28, 2026 14:12 UTC

This FAQ is provided for informational purposes only, reflects information available as of November 23, 2026, and does not amend or supplement your agreement with us or create additional obligations, representations, or warranties.