# Network Vulnerability Scanner Report

✔ 199.247.22.57

## Summary

**Overall risk level:**
High

**Risk ratings:**

| | |
|---|---|
| Critical: | 0 |
| High: | 1 |
| Medium: | 0 |
| Low: | 0 |
| Info: | 4 |

**Scan information:**

| | |
|---|---|
| Start time: | Nov 19, 2026 / 12:38:21 UTC+02 |
| Finish time: | Nov 19, 2026 / 12:38:34 UTC+02 |
| Scan duration: | 13 sec |
| Tests performed: | 7 |
| Scan status: | Finished |

## Findings

### nginx2root - nginx Remote Code Execution (CVE-2026-123007)

port 18443/tcp

CONFIRMED

We managed to detect this vulnerability using the following Request / Response chain.
We extracted the following information from the target: **nginx 1.31.8, HTTP/2 not confirmed**
Endpoint: **https://199.247.22.57:18443/**

Details

**Vulnerability description:**

nginx2root is a set of memory corruption bugs in nginx disclosed by Xint. The main one, CVE-2026-123007, is an integer underflow in HTTP/2 flow control accounting that leads to a heap buffer overflow in the worker process. The same release also fixes use-after-free bugs in HTTP/2 connection draining (CVE-2026-123633), the resolver (CVE-2026-123634), HTTP/3 (CVE-2026-121810) and the mail proxy auth_http path (CVE-2026-113425). nginx Open Source 0.5.33 to 1.30.6 and 1.31.0 to 1.31.8 is affected by at least one of these bugs, and the HTTP/2 overflow affects 1.9.5 and later. The fix is in 1.31.9 and 1.30.7. The template is a passive version check and sends no exploit trigger. It reads the nginx version from the Server header or from the default error page and reports affected versions. It also sends an HTTP/2 connection preface over cleartext TCP and notes in the result whether HTTP/2 is enabled. HTTP/2 over TLS needs ALPN, which the scanner cannot send, so on HTTPS ports HTTP/2 is reported as not confirmed.

**Risk description:**

An unauthenticated attacker can send crafted HTTP/2 traffic that corrupts the heap of an nginx worker, which can crash the worker or run code with its privileges. Xint chained this with a Linux kernel SCTP bug to get root on the host, including from inside a Docker container. The other bugs need HTTP/3, a resolver with a variable proxy_pass and mirror, or an exposed mail proxy. A match is based on the disclosed version. HTTP/2 is confirmed only on cleartext ports, and HTTP/3 and the mail proxy are not checked. Linux distributions backport fixes without changing the version, for example Ubuntu packages that still report 1.18.0 or 1.24.0, so a match should be confirmed against the installed package. The version disclosure is an exposure in its own right.

**Recommendation:**

Upgrade nginx to 1.31.9 or 1.30.7 or later, or install the patched package from your distribution, and restart nginx. Upgrade NGINX Plus as described in the F5 advisories. Until you can patch, disable HTTP/2 (http2 off; and remove http2 from listen lines) and HTTP/3 (remove quic listeners, http3 off;), use a fixed upstream instead of a variable proxy_pass where mirror is in use, and restrict mail proxy listeners to trusted networks. Set server_tokens off; to stop disclosing the version.

**References:**

https://nginx2root.com/
https://xint.io/blog/nginx2root-remote-code-execution
https://nginx.org/en/security_advisories.html
https://my.f5.com/manage/s/article/K000163926
https://my.f5.com/manage/s/article/K000163928
https://my.f5.com/manage/s/article/K000163925
https://my.f5.com/manage/s/article/K000163927
https://my.f5.com/manage/s/article/K000163931
https://ubuntu.com/security/notices/USN-8955-1
https://nvd.nist.gov/vuln/detail/CVE-2026-123007
https://www.cve.org/CVERecord?id=CVE-2026-123007

**Classification:**

CISA KEV: False
CVE : CVE-2026-123007
CVSS V3 : 8.1

## IP Information

CONFIRMED

| IP Address | Hostname | Location | Autonomous system (AS) Information | Organization (Name & Type) |
|---|---|---|---|---|
| 199.247.22.57 | 199.247.22.57.vultrusercontent.com | Frankfurt am Main, Hessen, Germany | The Constant Company, LLC (AS20473) | Vultr Holdings LLC Frankfurt (unknown) |

Details

**Risk description:**
If an attacker knows the physical location of an organization's IP address and its Autonomous System (AS) number, they could launch targeted physical or cyber attacks, exploiting regional vulnerabilities or disrupting critical infrastructure.

**Recommendation:**
We recommend reviewing physical security measures and monitoring network traffic for unusual activity, indicating potential cyber threats. Additionally, implementing robust network segmentation and adopting encryption protocols for data in transit can help protect sensitive information, even if attackers are aware of the IP addresses and the Autonomous System (AS) number.

## DNS Records

CONFIRMED

| Domain Queried | DNS Record Type | Description | Value |
|---|---|---|---|
| 199.247.22.57 | PTR | Pointer record | 199.247.22.57.vultrusercontent.com |

Details

**Risk description:**
An initial step for an attacker aiming to learn about an organization involves conducting searches on its domain names to uncover DNS records associated with the organization. This strategy aims to amass comprehensive insights into the target domain, enabling the attacker to outline the organization's external digital landscape. This gathered intelligence may subsequently serve as a foundation for launching attacks, including those based on social engineering techniques. DNS records pointing to services or servers that are no longer in use can provide an attacker with an easy entry point into the network.

**Recommendation:**
We recommend reviewing all DNS records associated with the domain and identifying and removing unused or obsolete records.

## Open ports discovery

CONFIRMED

| Port | State | Service | Product | Product Version |
|---|---|---|---|---|
| 18443 | open | None | - | - |

Details

**Risk description:**
This is the list of ports that have been found on the target host. Having unnecessary open ports may expose the target to more risks because those network services and applications may contain vulnerabilities.

**Recommendation:**
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

## OS Detection

UNCONFIRMED

| Operating System | Accuracy |
|---|---|
| Linux 3.10 - 4.11 | 94% |

Details

**Vulnerability description:**
OS Detection

## Scan coverage information

### List of tests performed (7)

**Port 18443**

✔ Checked for "nginx2root - nginx Remote Code Execution (CVE-2026-123007)"

**Generic tests**

✔ Performed DNS enumeration
✔ Performed IP information lookup phase
✔ Performed OS detection
✔ Performed port discovery
✔ Performed version-based engine detections
✔ Performed Nuclei engine detections

### Scan parameters

| | |
|---|---|
| Target: | 199.247.22.57 |
| Preset: | Custom |
| Scanning engines: | Nuclei |
| Check alive: | True |
| Extensive modules: | False |
| Protocol type: | TCP |
| Ports to scan: | 18443 |
| CVEs: | CVE-2026-123007 |
| Requests per second: | - |
| Scan CISA KEV only: | - |
| Fast mode: | - |