Government of Nepal
Office of the Prime Minister and Council of Ministers
Information Technology and Digital Governance Office
National Cyber Security Center
Singhadurbar, Kathmandu

Advisory Number: NCSC-1147-115-02 Date: 2083/08/03

साइबर सुरक्षा एडभाइजरी

हालै Java Programming Language सँग सम्बन्धित प्रणाली तथा Nginx प्रयोग गरि होस्ट गरिएका प्रणाली/सर्भरहरूमा क्रमशः Java4Shell र Nginx2Root गम्भीर सुरक्षा कमजोरीहरू पहिचान भएका छन्। यस्ता कमजोरीको दुरुपयोग भएमा सम्बन्धित प्रणाली तथा सर्भरमा अनधिकृत पहुँच प्राप्त हुने, सेवा अवरुद्ध हुने तथा प्रणालीमाथि पूर्ण नियन्त्रण कायम हुन सक्ने उच्च जोखिम रहन्छ। यसबाट बच्न देहाय बमोजिमका सुरक्षा उपायहरू तत्काल अवलम्बन गर्नुहुन सम्बन्धित सबै निकाय तथा प्रणाली सञ्चालकहरूमा अनुरोध छ।

1. Overview

Affected Technologies: Java Runtime Environment (JRE/JDK) and NGINX Web Server

Two critical security issues, Java4Shell (**CVE-2026-114938**) and NGINX2Root (**CVE-2026-123007, CVE-2026-123634, CVE-2026-123633, CVE-2026-121810, CVE-2026-113425**), have been publicly disclosed in November 2026.

- **Java4Shell:** A flaw in how OpenJDK (Java) decodes Base64 data. It can allow remote code execution or crash the application, but only on certain hardware.
- **NGINX2Root:** Five memory-handling flaws in the NGINX web server. An attacker could run code with the same privileges as the NGINX worker process.

2. Affected Systems and Products

A. Java4Shell (CVE-2026-114938)

Affected Java version	Minimum Fixed version
Java 8 Performance Build 8u511-perf	8u513
Java 17: 17.0.6–17.0.21	17.0.21.1
Java 21: 21.0.13 and earlier	21.0.13.1

Java 25: 25.0.5 and earlier	25.0.5.1
Java 27: 27.0.1 and earlier	27.0.1.1

- All OpenJDK-based distributions are affected (Oracle JDK, Temurin, Corretto, Azul Zulu, Microsoft, Red Hat, etc.).
- Applications that may be affected include Keycloak, Jenkins, Jira, Confluence and Artifactory.
- **Hardware condition:** The server must use an x86-64 processor with AVX-512 support (including VBMI), and attacker-controlled Base64 data must reach the decoder. ARM64 is not affected.

B. NGINX2Root

Five vulnerabilities are involved:

- CVE-2026-123007 – HTTP/2 memory corruption
- CVE-2026-123633 – HTTP/2 use-after-free
- CVE-2026-121810 – HTTP/3 use-after-free
- CVE-2026-123634 – Resolver use-after-free
- CVE-2026-113425 – Mail proxy use-after-free

Affected product	**Affected versions**	**Fixed version**
NGINX Open Source (stable)	1.30.6 and earlier	**1.30.7+**
NGINX Open Source (mainline)	Up to 1.31.8	**1.31.9+**
NGINX Plus	R34, R35, R36, R37 and affected releases	**37.0.8.1 or 37.3.0.1**, as applicable

- The flaws are in HTTP/2, HTTP/3, the resolver and mail proxy features, so exposure depends on which of these are enabled.
- NGINX is often built into other products (Kubernetes ingress controllers, OpenResty, Plesk), so check those too.
- Some Linux distributions fix the flaw without changing the version number, so confirm with your vendor.

3. Potential Impacts

Successful exploitation may result in:

- Remote Code Execution (RCE) and unauthorized server access.
- Exposure or theft of sensitive information and credentials.
- Memory corruption, application crashes and Denial of Service (DoS).
- Website defacement, service disruption and unauthorized modification of data.
- Further compromise of connected systems and internal networks.

4. How to Check Whether Systems Are Affected

For Java4Shell:

Execute the following commands on Linux systems:

```
java -version
grep -om1 -E 'avx512[_]?vbmi' /proc/cpuinfo
```

- The first command shows your Java version. Compare it to the table above, and check Java bundled inside applications and containers.
- If the second command returns a result, the CPU supports the feature that makes the flaw exploitable.

For NGINX2Root:

```
nginx -v
nginx -V 2>&1
nginx -T 2>&1 | grep -Ei 'http2|http3|quic|resolver|mirror|auth_http'
```

These show your NGINX version, how it was built, and whether the risky features are enabled. Also check NGINX running in containers, Kubernetes and third-party products.

5. Recommended Mitigation and Remediation

Java4Shell:

1. Upgrade affected Java installations to the corresponding fixed versions.
2. For other OpenJDK distributions, install the vendor's corresponding security-patched release.
3. If immediate upgrading is not possible, temporarily disable the vulnerable Base64 intrinsic.
4. Restart all affected Java applications after applying the update or mitigation.

NGINX2Root:

1. Immediately upgrade NGINX Open Source to **1.30.7 (stable)** or **1.31.9 (mainline)**, or install the applicable fixed NGINX Plus release.
2. Update embedded NGINX components and container images through their respective vendors.
3. If you can't patch right away, temporarily disable HTTP/2 and HTTP/3, and turn off resolver, mirror and mail proxy features you don't need. This lowers risk but is **not a substitute for patching**.
4. Restart or reload NGINX and confirm the patched version is running.

6. Action Required

All government agencies, organizations and operators of critical information infrastructure are requested to:

- Find all systems running affected Java and NGINX versions.
- Fix internet-facing, login and business-critical systems first.
- Apply updates and confirm they installed correctly.
- Watch logs for unusual activity, unexpected processes and unexplained crashes.
- Report suspected attacks to the National Cyber Security Center (NCSC).

References:

- OpenJDK: https://openjdk.org/groups/vulnerability/advisories/2026-11-17
- NGINX: https://nginx.org/en/security_advisories.html
- Java4Shell: https://calif.io/java4shell/
- NGINX2Root: https://nginx2root.com
- https://securitylabs.datadoghq.com/articles/java4shell-remote-code-execution-in-openjdk-cve-2026-114938/