GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

4 September 2026

Advisory 253: GeoNetwork Remote Code Execution via Unsafe XSLT Processor Configuration (CVE-2026-58400).

Release Date: 3rd September 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, System/Network administrators, and geospatial/GIS teams that deploy or operate GeoNetwork as a metadata catalog or spatial data infrastructure (SDI) platform, including government geoportal backends. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-58400 is a critical remote code execution vulnerability in GeoNetwork, an open-source geospatial metadata catalog maintained under the OSGeo Foundation and widely used to power Spatial Data Infrastructure (SDI) deployments and government geoportals worldwide - the reporting researchers' own internet-wide scan fingerprinted 121 internet-exposed instances across 39 countries, 89% of which were government, military, or national-agency deployments.

What are the systems affected?

The following version(s) are affected:

- GeoNetwork 4.3.0 up to (but not including) 4.4.12 - (Affected)
- GeoNetwork before 4.2.17 - (Affected)

GeoNetwork 4.4.12 and 4.2.17, and later on each respective branch - (Not affected, patched)

GeoNetwork is typically self-hosted rather than centrally updated by the vendor, so this fix will not reach an existing deployment on its own.

What does this mean?

Typical attack flow:

1. **Obtain formatter-upload access, directly or via the companion vulnerability**
    - An attacker who holds a GeoNetwork account with formatter-upload privileges — or who instead exploits the separate, unauthenticated formatter-upload vulnerability tracked as CVE-2026-63219 — uploads a malicious .xsl or .zip formatter file to the server.
2. **Trigger the malicious formatter to execute arbitrary commands**
    - The attacker requests a metadata record using the malicious formatter, for example via a crafted GET request. Because GeoNetwork's Saxon XSLT processor does not enable secure processing, the formatter's stylesheet code can invoke Java methods such as Runtime.exec() or ProcessBuilder directly, executing arbitrary operating-system commands as the GeoNetwork process user.

Attack vectors:

- A network-based attack requiring the attacker to already hold formatter-upload privileges on a reachable GeoNetwork instance (CVSS PR:H) — or, when chained with CVE-2026-63219's missing authorization check, no privileges at all.
- No user interaction is required (CVSS UI:N). CERTVU is not aware of confirmed active exploitation at the time of writing, but a researcher-run internet-wide scan found 121 vulnerable, internet-exposed instances, predominantly government and national-agency systems, underscoring the real-world exposure.

Successful exploitation may allow attackers to:

- Execute arbitrary operating-system commands on the server hosting GeoNetwork, achieving full remote code execution as the GeoNetwork process user.
- Access, exfiltrate, or tamper with the geospatial metadata catalog and any other data reachable from the compromised host, and use the compromised server as a foothold into other government or agency network segments — a particular concern given the documented majority-government exposure worldwide.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Upgrade GeoNetwork to version 4.4.12 or 4.2.17 (whichever branch applies) or later, where this vulnerability is fixed (GitHub Security Advisory GHSA-x898-729x-cc3r). Fixed releases

have been available since 8 July 2026, ahead of this CVE's public disclosure, so an unpatched instance has had time to apply the update.

2. Treat internet-exposed instances as a priority, given documented evidence that most publicly-reachable GeoNetwork instances worldwide belong to government and national-agency operators
3. Restrict who can upload formatters
4. Audit the estate for GeoNetwork deployments
5. Review formatter uploads and access logs

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-58400
2. https://github.com/geonetwork/core-geonetwork/security/advisories/GHSA-x898-729x-cc3r