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

31 August 2026

Advisory 214: Oracle Reports Developer Multiple Vulnerabilities (CVE-2026-62613, CVE-2026-62637, CVE-2026-70670).

Release Date: 24th August 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 and System/Network administrators that operate Oracle Fusion Middleware, in particular Oracle Reports Developer. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-62613, CVE-2026-62637 and CVE-2026-70670 are critical vulnerabilities in the Security and Authentication component of Oracle Reports Developer, part of Oracle Fusion Middleware. Each is easily exploitable by an unauthenticated attacker who has access to the same physical or adjacent network segment as the hardware running Oracle Reports Developer.

Successful exploitation lets an attacker compromise Oracle Reports Developer over the network without needing valid credentials or any user interaction. Because the vulnerabilities carry a "Scope: Changed" rating, a successful attack can affect resources beyond Reports Developer itself, including other components that rely on it within the same Fusion Middleware deployment.

What are the systems affected?

The following version(s) are affected:

- Oracle Reports Developer 12.2.1.19.0 (affected by CVE-2026-62613) – (Affected)
- Oracle Reports Developer 14.1.2.0.0 (affected by CVE-2026-62637 and CVE-2026-70670) – (Affected)

There is no separate patched product version; Oracle addresses these flaws through security patches rather than a version upgrade.

Administrators should confirm their Oracle Reports Developer build number against Oracle's August 2026 Critical Security Patch Update (CPU) risk matrix and apply the corresponding patch through My Oracle Support.

What does this mean?

Typical attack flow:

1. **Network positioning**
    - An attacker gains access to the physical or adjacent network segment that the Oracle Reports Developer server is attached to (for example, an internal LAN segment, VLAN, or a compromised device on the same network).
2. **Unauthenticated exploitation**
    - The attacker sends crafted requests to Reports Developer's Security and Authentication component without needing any credentials or user interaction, compromising confidentiality and integrity of the product and any connected resources.

Attack vectors:

- Access to the same physical or adjacent network segment as the Reports Developer host (no direct internet exposure required).
- Lateral movement from an already-compromised device or user workstation on the same segment.

Successful exploitation may allow attackers to:

- Create, modify, or delete data accessible to Oracle Reports Developer.
- Extend impact beyond Reports Developer to other Fusion Middleware components sharing the same deployment, given the "Scope: Changed" nature of the flaws.

Mitigation process

CERTVU recommends the following:

1. Apply Oracle's August 2026 Critical Security Patch Update

- Identify all Oracle Reports Developer / Fusion Middleware instances (versions 12.2.1.19.0 and 14.1.2.0.0) and apply the patches listed for CVE-2026-62613, CVE-2026-62637 and CVE-2026-70670 in Oracle's August 2026 Critical Security Patch Update.

2. Restrict network access to the Reports Developer segment
3. Segment and monitor the network

- Place Oracle Reports Developer hosts on a restricted VLAN or segment, limiting adjacent-network access to trusted administrative systems only, and monitor for anomalous traffic to the Reports Developer service.

4. Audit the estate for the affected product

- Confirm whether any business system depends on the affected Reports Developer instance and assess exposure of connected data before and after patching.

5. Monitor Oracle's security advisories page for further updates

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

Reference

1. https://www.oracle.com/security-alerts/cspuaug2026.html
2. https://www.cve.org/CVERecord?id=CVE-2026-62613
3. https://www.cve.org/CVERecord?id=CVE-2026-62637
4. https://www.cve.org/CVERecord?id=CVE-2026-70670