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

25 August 2026

Advisory 196: CVE-2026-21962_Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability

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 utilize the above products. This alert is intended to be understood by technical users and systems administrators.

Who should take note?

Oracle HTTP Server and the Oracle WebLogic Server Proxy Plug-in are components of Oracle Fusion Middleware. They are enterprise-tier products, so the number of deployments in Vanuatu is expected to be small, but those most likely to operate them are high-value organisations:

- Banking and financial institutions, including core banking and internet banking platforms
- Telecommunications operators and Internet Service Providers
- Government agencies operating Oracle-based financial management, revenue or customs systems
- Any organisation running Java enterprise applications behind Oracle HTTP Server, or an Apache or IIS front end using the WebLogic proxy plug-in

CERTVU advises organisations in these sectors to confirm, with their own IT teams and with any external systems integrator or application vendor, whether Oracle Fusion Middleware is in use and whether the January 2026 Critical Patch Update has been applied.

What is it?

CVE-2026-21962 is a maximum-severity improper access control vulnerability (CWE-284) affecting Oracle HTTP Server and the Oracle WebLogic Server Proxy Plug-in for Apache HTTP Server and Microsoft IIS. It carries a CVSS v3.1 Base Score of 10.0, the highest possible rating.
The flaw arises from improper handling of incoming requests by the proxy plug-in. A remote, unauthenticated attacker with network access over HTTP can send crafted requests that bypass intended access restrictions, resulting in unauthorised access to critical data and unauthorised creation, deletion or modification of that data. No credentials and no user interaction are required, and attack complexity is low.
CERTVU is issuing this advisory now because the vulnerability has since been confirmed exploitation in the wild.

What are the systems affected?

Affected systems are Oracle HTTP Server and Oracle WebLogic Server Proxy Plug-in deployments for Apache HTTP Server and Microsoft IIS.

Oracle HTTP Server / WebLogic Server Proxy Plug-in 12.2.1.4.0 - (Affected)
Oracle HTTP Server / WebLogic Server Proxy Plug-in 14.1.1.0.0 - (Affected)
Oracle HTTP Server / WebLogic Server Proxy Plug-in 14.1.2.0.0 - (Affected)
Versions with the Oracle January 2026 Critical Patch Update applied - (Not affected, patched)

Organisations should verify affected versions against Oracle's own January 2026 Critical Patch Update advisory, which is the authoritative source for the full list of affected products and required patches.

What does this mean?

CERTVU draws particular attention to the age of this vulnerability. It was patched by Oracle seven months ago, in January 2026.
Oracle Fusion Middleware updates are frequently deferred because they are disruptive and often require the involvement of a systems integrator or application vendor. That is precisely why a vulnerability of this age continues to have victims.

Step 1 - Unauthenticated Network Access
The attacker requires only HTTP access to the affected proxy component. Because these plug-ins front-end web applications, they are commonly positioned in DMZ environments and reachable from the internet by design.

Step 2 - Access Control Bypass (CVE-2026-21962)
The attacker sends crafted HTTP requests that are improperly handled by the proxy plug-in, bypassing the access restrictions intended to protect the backend application.

Step 3 - Unauthorised Data Access and Modification
The attacker gains unauthorised access to critical data handled by the server, and the ability to create, delete or modify that data.

Step 4 - Propagation Across the Middleware Stack
Because the vulnerability carries a scope change, impact is not confined to the proxy component. Backend WebLogic Server instances and the applications and data they serve may be affected through the compromised conduit.

CERTVU notes that a number of publicly circulating technical write-ups and proof-of-concept scripts for this vulnerability contain contradictory and unverified descriptions of the exploitation mechanism. Organisations should base their assessment and remediation on Oracle's own Critical Patch Update advisory rather than on third-party analysis.

Mitigation process

CERTVU recommends the following:

1. **Determine Whether Oracle Fusion Middleware Is Present**

Establish first whether your organization operates Oracle HTTP Server or the WebLogic Server Proxy Plug-in at all, including instances deployed and maintained by an external systems integrator or application vendor. Where an application is supplied and supported by a third party, ask that party directly whether the January 2026 Critical Patch Update has been applied.

2. **Apply the Oracle January 2026 Critical Patch Update**

Apply the Oracle January 2026 Critical Patch Update to all affected versions.

3. **Restrict Exposure Where Patching Is Delayed**

Where the update cannot be applied immediately because of vendor dependencies or change control, restrict access to the affected component to trusted networks, and apply web application firewall inspection of HTTP traffic to the proxy component as an interim compensating control. These are mitigations, not remediation, and the update remains necessary.

4. **Report**

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

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-21962
2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3. https://nvd.nist.gov/vuln/detail/CVE-2026-21962
4. https://cwe.mitre.org/data/definitions/284.html