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

27 August 2026

Advisory 198: CVE-2021-23758_Ajax.NET Professional Deserialization of Untrusted Data Vulnerability

Release Date: 26th August 2026
Impact: HIGH
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.

What is it?

CVE-2021-23758 is a deserialization of untrusted data vulnerability (CWE-502) affecting all versions of the Ajax.NET Professional (AjaxPro) library for Microsoft .NET. It carries a CVSS Base Score of 9.8 and can allow remote code execution on the affected web server.
The library fails to restrict which .NET class types may be created during deserialization. An attacker who submits a specially crafted serialized .NET object to an AjaxPro endpoint can therefore cause the server to instantiate a class of the attacker's choosing, and through that, execute arbitrary commands with the privileges of the web application.
CERTVU draws particular attention to the fact that the affected component is end-of-life.

What are the systems affected?

ASP.NET web applications that include the Ajax.NET Professional library, hosted on Microsoft Internet Information Services (IIS) or equivalent.

All versions of the AjaxPro and AjaxPro.2 packages - (Affected)
No supported fixed version is available - (End-of-life)

The vulnerability affects the library, not a specific product, so exposure depends entirely on whether an individual application includes it.

Because AjaxPro is an embedded component rather than an installed product, organisations must inspect their web applications directly. CERTVU recommends the following checks on each web server:

1. Search the web application directories for the library files:
```
dir /s /b C:\inetpub\*AjaxPro*.dll
```

2. Inspect each application's web.config file for a registered AjaxPro handler, typically appearing as a handler or httpHandler entry referencing AjaxPro or the path ajaxpro/*.ashx.

3. Test whether an AjaxPro endpoint responds on the application, by requesting a path of the form:
```
https://<application>/ajaxpro/
```

Organisations should carry out these checks on internal applications as well as internet-facing ones.

What does this mean?

Step 1 - Endpoint Discovery
The attacker identifies a web application exposing an AjaxPro endpoint. Endpoints are typically reachable under an ajaxpro path and are visible in the application's client-side code.

Step 2 - Crafted Serialized Object
The attacker submits a serialized .NET object specifying a class type of their choosing, rather than the type the application expects.

Step 3 - Insecure Deserialization (CVE-2021-23758)
Because the library does not restrict permitted types, the server instantiates the attacker-specified class during deserialization.

Step 4 - Remote Code Execution
The instantiated class is used to execute operating system commands with the privileges of the web application process, giving the attacker a foothold on the web server.

CERTVU notes an important qualification. Independent analysis indicates that this vulnerability is not readily exploitable by an attacker with no prior knowledge of the target application, because a working payload requires knowledge of the application-specific method and object names.

Mitigation process

CERTVU recommends the following:

1. **Determine Whether the Component Is Present**

Carry out the checks set out above across all web applications, internal and internet-facing, and engage any external contractor responsible for those applications. Until this is done, an organisation cannot know whether it is affected.

2. **Remove the Component**

Where AjaxPro is present, the definitive remediation is to remove the library from the application and refactor the affected functionality to use a supported framework. There is no patched version, so this is a development task rather than a patching task and should be scheduled accordingly with the application owner or vendor.

Other options include;

- Block the Endpoint as an Interim Control
- Restrict Exposure and Reduce Privilege
- Consider Retiring the Application
- Review for Prior Compromise

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

Reference

1. https://www.cve.org/CVERecord?id=CVE-2021-23758
2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3. https://nvd.nist.gov/vuln/detail/CVE-2021-23758
4. https://cwe.mitre.org/data/definitions/502.html