EXPLOITED VULNERABILITY ADVISORY: CVE-2021-23758

Summary

CVE-2021-23758 in Ajax.NET Professional Ajax.NET Professional is being actively exploited in the wild. All versions of package ajaxpro.2 are vulnerable to Deserialization of Untrusted Data due to the possibility of deserialization of arbitrary .NET classes, which can be abused to gain remote code execution. CISA requires federal remediation by 2026-09-09; under the CRA, exploitation of an affected product must be reported within 24 hours.

What we know

- **CVE:** CVE-2021-23758
- **Affected:** Ajax.NET Professional Ajax.NET Professional
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-26
- **Severity:** CVSS 8.1 High, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 84%
- **Weakness:** CWE-502

Recommended action

Patch CVE-2021-23758 by 2026-09-09. If you cannot patch immediately, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. If you ship an affected product, be ready to file the CRA 24-hour report the moment you find it exploited.

Sources: CISA Known Exploited Vulnerabilities, NIST NVD. Public data; an advisory of active exploitation, not an incident report. Verify applicability to your estate before acting.