N2SEC Security Advisories

Official advisories, vulnerability disclosures, and cybersecurity alerts

About

N2 Cybersecurity Consulting Inc. publishes verified security advisories and vulnerability alerts to help organizations stay informed and protected against emerging threats. Each advisory provides *technical details, risk assessments, and recommended mitigation actions.*

All advisories follow recognized industry disclosure standards and are labeled according to the **Traffic Light Protocol (TLP)** to indicate information sharing restrictions.

Recent Advisories

Advisory ID	Title	Date	Severity	TLP
N2SA-2025-003	Oracle E-Business Suite Remote Code Execution (CVE-2025-61882)	Oct 8, 2025	**Critical (9.8)**	TLP:CLEAR
N2SA-2025-002	Microsoft Exchange security advisory (AV25-490)	Aug 7, 2025	**High (8.0)**	TLP:CLEAR
N2SA-2025-001	Microsoft SharePoint Server (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770)	July 15, 2025	**Critical (9.8)**	TLP:CLEAR

Recommended Mitigation Steps

- Apply security updates for each CVE listed immediately.
- Restrict or remove public internet exposure where feasible.
- Enforce network segmentation and consider Web Application Firewall (WAF) protections.
- Monitor for Indicators of Compromise (IOCs) and unusual HTTP request activity.
- Conduct targeted log review and vulnerability scans to detect potential exploitation.
- Review and follow Oracle’s and Microsoft's official advisories and any updated guidance.

About N2SEC Advisories

N2 Cybersecurity Consulting Inc. issues public advisories to promote awareness, readiness, and resilience across industries. Our analyses are based on vendor disclosures, open-source intelligence (OSINT), and independent assessment.

Contact: contact@n2sec.ca
Website: https://n2sec.ca

Information Security Advisory | TLP:CLEAR