AYI NEDJIMI Consultants

Attaques SAML 2026 : Golden SAML, XSW & Défense IdP

16 mai 2026 • Mis à jour le 17 mai 2026 • 18 min de lecture • 3702 mots • 18 vues •

À retenir — Attaques SAML 2026 Les attaques SAML ciblent le maillon faible de la fédération d'identité : la signature XML, la confiance IdP→SP et la session.

À RETENIR

À retenir — Attaques SAML 2026

Les attaques SAML ciblent le maillon faible de la fédération d'identité : la signature XML, la confiance IdP→SP et la session post-authentification.

Trois familles : Golden SAML (forge complète
IdP volé), XSW (XML Signature Wrapping, ma

structure), account takeover via IdP malveillant (CVE-2026-42354 Sentry, CVE-2026-41103 Atlassian).

Détection : alerte sur SAML Response avec *NotOnOrAfter* > 24h, signatures multiples, IdP différent du tenant attendu, claims *impersonation*.

Défense : rotation tokens IdP courte (max 1h), audit ADCS et ADFS, monitoring AD CS via Sysmon Event ID 4886 + 70, séparation tier IdP signing key.

Cas réels : SolarStorm/Nobelium (2020-2024), CVE-2026-3055 Citrix NetScaler, CVE-2026-41103 Jira/ Confluence, CVE-2026-42354 Sentry SAML SSO.

Les **attaques SAML** sont l'un des vecteurs d'*account takeover* les plus rentables pour les attaquants en 2026. Le protocole SAML 2.0, standardisé en 2005 par OASIS, reste la colonne vertébrale de l'authentification fédérée d'entreprise — il transporte assertions XML signées entre un *Identity Provider* (Microsoft ADFS, Entra ID, Okta, OneLogin, PingFederate, Keycloak) et des *Service Providers* (Salesforce, AWS, GitHub Enterprise, Atlassian, Workday, et des milliers de SaaS). Une attaque réussie sur la couche SAML donne un **accès persistant et silencieux** à des dizaines d'applications critiques — souvent indétectable côté SOC car les logs SP montrent une authentification SAML normale. Ce panorama 2026 couvre les trois familles d'attaques (Golden SAML, XSW, IdP compromis ou malveillant), les CVE 2026 majeures, les techniques d'investigation forensique, et les défenses concrètes pour ADFS, Entra ID, Okta, Keycloak.

Réponse sous 24h

Devis gratuit →