Clutch Security Uncovers Critical OneLogin API Vulnerability Exposing Secrets

CVE-2025-59363 vulnerability allowed unauthorized access to OIDC client secrets across 110,000+ applications, creating supply chain risks for 5,500+ enterprises

Clutch Security

TEL AVIV, ISRAEL, October 1, 2025 /EINPresswire.com/ -- Clutch Security Discovers Critical Vulnerability in OneLogin's API That Exposed Enterprise Authentication Credentials

Security researchers at Clutch identified CVE-2025-59363, a high-severity flaw enabling attackers to access sensitive client secrets through standard API calls

> This vulnerability demonstrates how identity provider compromises can cascade across entire business ecosystems, creating supply chain attack opportunities."
>
> *Ofir Har-Chen*

TEL-AVIV, ISRAEL – October 1, 2025 – Clutch Security, a leading cybersecurity startup, today disclosed the discovery of a critical vulnerability in OneLogin's API that exposed sensitive OpenID Connect (OIDC) application client secrets. The vulnerability, tracked as CVE-2025-59363 with a CVSS score of 7.7 (High severity), affected an estimated 110,000 to 275,000 OIDC applications across OneLogin's 5,500+ enterprise customers globally.

The vulnerability allowed any actor with valid OneLogin API credentials to enumerate and retrieve client secrets for all OIDC applications within an organization's tenant. This created a significant supply chain risk, where a single set of compromised vendor credentials could expose an organization's entire OIDC application portfolio.

The Supply Chain Attack Multiplier:
The vulnerability's impact extended far beyond typical security flaws due to common enterprise practices around credential sharing. Organizations routinely share OneLogin API keys with third-party vendors for integration purposes. Due to OneLogin's role-based access control model, these API keys typically have broad access to all endpoints.

"This vulnerability demonstrates how identity provider compromises can cascade across entire business ecosystems," said Tal Kimhi, VP R&D at Clutch Security. "A vendor with legitimate API access for one specific integration could inadvertently expose credentials for dozens of critical applications across the organization's infrastructure."

With exposed client secrets, attackers could impersonate legitimate applications and perform OAuth flows to obtain access tokens, effectively bypassing authentication controls for integrated services including cloud infrastructure platforms, databases, financial systems, and business-critical applications.
Technical Overview

The vulnerability existed in OneLogin's /api/2/apps endpoint, designed to list applications configured within a tenant. While this endpoint should return only metadata and public identifiers, it inadvertently included sensitive client_secret values in plaintext within the API response.

The exploitation process required only two simple steps:

Authenticate using valid OneLogin API credentials via standard OAuth2 client credentials flow
Query the /api/2/apps endpoint to retrieve the application list containing exposed client secrets
Notably, OneLogin does not support IP address restrictions for API access, meaning attackers could exploit the vulnerability from anywhere globally, and organizations had no mechanism to limit API key usage by geographic location.

Who Was Affected:
The vulnerability impacted OneLogin customers meeting the following criteria:

- Organizations with OpenID Connect applications configured in their OneLogin tenant
- Companies that provided OneLogin API keys to third-party vendors, contractors, or internal teams
- Enterprises relying on OneLogin's standard RBAC model with broad endpoint access

This combination is extremely common in enterprise environments where OneLogin serves as a central identity provider for multiple integrations. Based on industry patterns, this likely affected the vast majority of OneLogin's enterprise customer base.

Responsible Disclosure and Resolution:
Clutch Security identified the vulnerability during routine security assessments of identity provider APIs in July 2025. Upon discovery, the team immediately recognized the severity given OneLogin's widespread enterprise adoption and potential for credential sharing scenarios to amplify impact.
The company followed responsible disclosure practices:

July 18, 2025: Initial vulnerability report submitted to OneLogin
July 22, 2025: OneLogin acknowledged and classified as Critical
July 30, 2025: OneLogin confirmed vulnerability and committed to resolution
September 9, 2025: OneLogin confirmed vulnerability resolution in version 2025.3.0
September 10, 2025: Clutch validated and confirmed the fix
September 15, 2025: OneLogin provided CVE reference and official statement

OneLogin responded professionally throughout the disclosure process and provided the following statement:
"Protecting our customers is our top priority, and we appreciate the responsible disclosure by Clutch Security. The reported vulnerability was resolved with the OneLogin 2025.3.0 release. To our knowledge, no customers were impacted by this vulnerability." — Stuart Sharp, VP of Product, OneLogin

Clutch Security found no evidence of active exploitation, and OneLogin confirmed that no customers were impacted during the vulnerable period.
Immediate Actions Required

Organizations using OneLogin with OIDC applications should take the following steps:
Verify their OneLogin tenant is running version 2025.3.0 or later
Regenerate client secrets for all OIDC applications as a precautionary measure
Monitor logs for unusual authentication patterns or unexpected application access
Audit API usage logs to verify access patterns align with expected vendor locations

Key Security Implications:
This discovery underscores several critical considerations for enterprise identity management:
- API Security as Foundation Security: Identity providers serve as the backbone of enterprise security architecture. Vulnerabilities in these systems can have cascading effects across entire technology stacks.
- Credential Sharing Amplifies Risk: While sharing API credentials with trusted vendors is often necessary, organizations must understand this practice can amplify vulnerability impacts far beyond originally intended scope.
- Principle of Least Privilege: Organizations should advocate for more granular permission models and regularly audit the scope of shared credentials.
- Supply Chain Security Vigilance: Identity provider compromises can cascade across vendor relationships, creating supply chain attack opportunities that extend far beyond direct vendor access.

Upon confirming the vulnerability resolution, Clutch immediately notified customers using OneLogin in their environments, providing detailed remediation steps and timeline for public disclosure.

About Clutch Security
Clutch Security is the leader in the Non-Human Identity Security, working with enterprises to secure their machine identities with their Universal NHI Security platform.
For more information about CVE-2025-59363, including technical details and proof of concept, visit the full blog post at https://www.clutch.security/blog/onelogin-many-secrets-clutch-uncovers-vulnerability-exposing-client-credentials.

Ofir Har-Chen
Clutch Security
email us here
Visit us on social media:
LinkedIn
