RESEARCH

Research is one of our founding principles and we invest in it heavily. All of our researchers have the privilege to use 25% of their time exclusively for self-directed research.

By discovering new vulnerabilities and attack techniques, we are constantly improving our capabilities and contributing to the security of the digital world.

BLOG GITHUB ABOUT DOYENSEC

ALL PUBLICATION (39) BLOG (76) ADVISORY (47) CODE (20)

Search for posts

10/27/2026

ElectroNG is now open-source!

CODE

ElectroNG is a tool for analyzing the security of ElectronJS applications. It allows security researchers to quickly identify potential security issues in ElectronJS apps, such as insecure `webPreferences` settings, unsafe preloads, and other common pitfalls.

10/13/2026

Playing It SFAPE: Code Execution in Isolated User Mode

BLOG

Doyensec discovered multiple vulnerabilities in `SFAPE.dll`, a VBS enclave shipped with Windows, and chained them to gain code execution within the enclave in Windows Isolated User Mode (VTL1). The post explores how VBS enclaves work and how memory

09/24/2026

One Tap Too Far: Using Shortcuts to Bypass Chrome for iOS Call Prompts

BLOG

Doyensec identified a vulnerability in Chrome for iOS that allowed a malicious webpage to bypass the browser's app-launch protections by leveraging the trusted `shortcuts://` and `workflow://` URL schemes. By supplying an attacker-controlled `x-error` to the

09/17/2026

The skb that wasn't freed - the Fragnesia

We discovered a deterministic local privilege escalation vulnerability affecting the default install of the latest Arch, Fedora, Debian, Amazon Linux and RHEL distributions, having unprivileged user namespaces enabled, `openvswitch` auto-loading, and a stock kernel carrying

primitive via Open vSwitch

BLOG

07/27/2026

ElectronJS - shell.openPath Path Validation Bypass via Embedded Null Byte

Doyensec identified a security issue affecting the ElectronJS framework. The `shell.openPath()` API did not reject file paths containing embedded null bytes, allowing string-based path validation (such as file extension allow-lists) to be silently bypassed and a different file to be opened

ADVISORY

07/01/2026

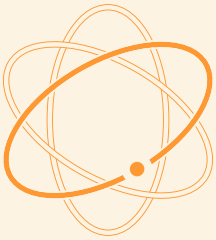
Fider - SSRF in OAuth URLs, Cross-Tenant Invitation Acceptance

Doyensec identified two security issues affecting the Fider web application. A user-controlled OAuth URLs allowed for Server-Side Request Forgery (SSRF) on the target deployment, and a cross-tenant invitation acceptance vulnerability, leading to unauthorized access

ADVISORY

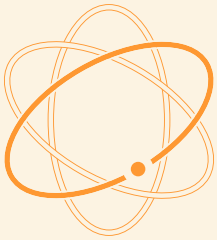
SHOW MORE

OUR PUBLIC TOOLS



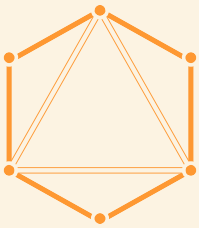
ELECTRONG

Premium ElectronJS Security Scanning Tool



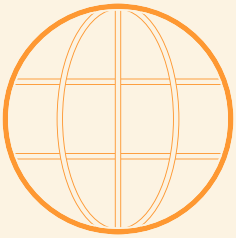
ELECTRONEGATIVITY

OpenSource ElectronJS Security Scanning Tool



INQL

GraphQL Security Testing Tool



BURP-REST-API

Rest/JSON API for Burp Suite

DOYENSEC

US OFFICE

350 Townsend Street, Suite 840
San Francisco, CA 94107 - USA

EMEA OFFICE

Via Ventotto Luglio n. 212 - Borgo Maggiore
47893 Repubblica di San Marino

FOR PROPOSALS OR QUESTIONS

info@doyensec.com or +1 (628) 333 9093

© 2017-2026 Doyensec LLC.