BALDUR.

GOOGLE CHROME

Google Chrome

Prepared for Google Chrome

Table of contents

01 Findings 3

Findings

This table provides a comprehensive list of all findings discovered during the assessment. Each item is categorized and listed by severity, allowing for quick identification of the most critical issues. The entries are interactive, enabling you to click on any finding to navigate directly to detailed information for further analysis and resolution.

#	Title	Severity
1	Video Picture In Picture as fake login box	CRITICAL

#1: Video Picture In Picture as fake login box	
Severity	Critical
Component	Video tag Picture in Picture

Description

A vulnerability in Google Chrome's Picture-in-Picture (PiP) feature allows an attacker to display a persistent, fake authentication prompt—mimicking trusted interfaces like Apple's login or Okta's password box. This is done by having a video that looks exactly like a login box which does not show the origin. The main window will pickup the keystrokes. Although PiP requires user activation, the nearly 5-second timeout on transient activation (https://developer.mozilla.org/en-US/docs/Glossary/Transient_activation) can be exploited to show the deceptive popup while the user is on a completely different workspace. You can use the `blur` event to detect this.

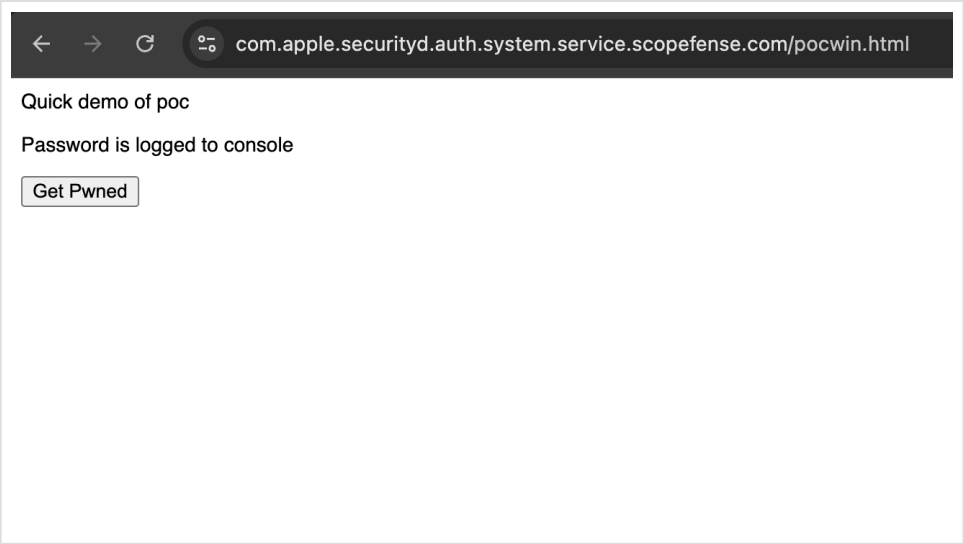
https://developer.mozilla.org/en-US/docs/Web/API/DocumentPictureInPicture/requestWindow

System Details

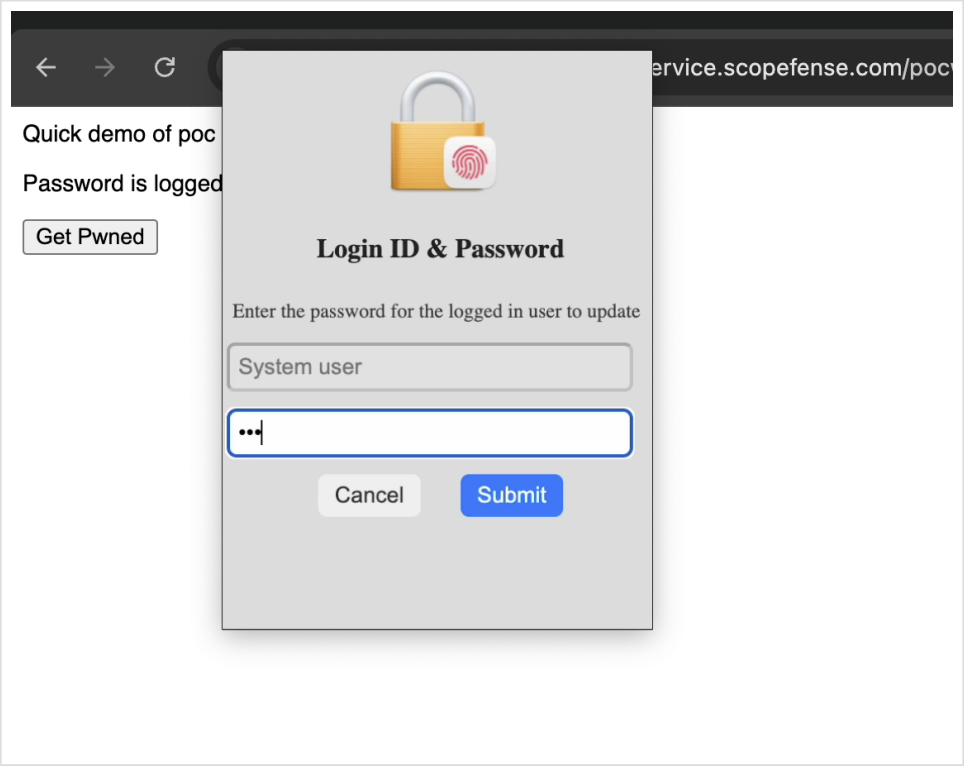
Version tested: Version 131.0.6778.265 (Official Build) (arm64)
OSX: Sonoma 14.5 Macbook Pro M3

Proof of concept

1. Visit https://com.apple.securityd.auth.system.service.scopefense.com/pocwin.html
2. Click **Get pwned** (This could be any normal activity that triggers the transient activation)



3. The victim is likely to trust the prompt—believing it to be a legitimate out-of-browser request—and may enter credentials that can be stolen.



When they enter the password the video src tag will be switched everytime so it looks like a correct password entry. Since the video tag listens for enter tag to close the box, it will close when people click enter. The domain name does not matter as it is never shown

Video of the attack is provided here: https://drive.proton.me/urls/KASADP51V8#Ma54GF0Ida1b

Impact

Users typically recognize legitimacy through persistent, out-of-browser popups. This vulnerability undermines that assurance, enabling attackers to create convincing fake login

interfaces (such as OKTA, Google Auth, or 2FA prompts) with minimal visible indicators of their true origin.

Remediation

Origin needs to be shown on video boxes as they can resemble web pages. Furthermore the transient keys should switch to sticky keys.