CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

09 May 2024

VPN TunnelVision Vulnerability

CVE-2024-3661 | TunnelVision | VPN | High Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high vulnerability known as CVE-2024-3661.[1] The vulnerability affects computers connected to a Virtual Private Network (VPN) through untrusted networks.[2] Exploitation of CVE-2024-366 may allow an attacker on the same local network, to route traffic through an unencrypted tunnel and collect some or all of the data. The VPN application will report that all data is being sent through the protected connection. Any traffic that's diverted away from this tunnel will not be encrypted by the VPN and the Internet IP address viewable by the remote user will belong to the network the VPN user is connected to, rather than one designated by the VPN app.[3,4]

The Cal-CSIC recommends to not use untrusted networks (Public WiFi), consider using a hotspot with your VPN, consider using a VPN inside a virtual machine that does not have a bridged network adapter, and to use AdBlock and privacy browsers that reject tracking cookies.

For further information on the vulnerability and mitigation recommendations, please refer to [TunnelVision].

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Leviathan Security Group; "TunnelVision;" https://www.leviathansecurity.com/research/tunnelvision; accessed 09 May 2024

[2] Kerbs On Security; "Why Your VPN May Not Be As Secure As It Claims;" https://krebsonsecurity.com/2024/05/why-your-vpn-may-not-be-as-secure-as-it-claims/; accessed 09 May 2024

[3] Ars Technica; "Novel attack against virtually all VPN apps neuters their entire purpose;" https://arstechnica.com/security/2024/05/novel-attack-against-virtually-all-vpn-apps-neuters-their-entire-purpose/; accessed 09 May 2024

[4] National Vulnerability Database; "CVE-2024-3661 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-3661; accessed 09 May 2024

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.