Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
30 April 2024

DMitry Vulnerability

CVE-2024-31837 | DMitry | Buffer Overflow | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-31837.[1] The vulnerability affects DMitry (Deepmagic Information Gathering Tool) version 1.3a. Dmitry is a UNIX/(GNU)Linux command line application written in C. DMitry can find possible subdomains, email addresses, uptime information, perform tcp port scan, whois lookups, and more.[2] Exploitation of the buffer overflow vulnerability may allow an attacker to cause a denial of service (application crash) or possibly have unspecified other impact via a long argument.[3]

The Cal-CSIC recommends applying DMitry format string and buffer overflow fixes as soon as possible.

For further information on applying DMitry fixes, please refer to GitHub DMitry fixes #12.

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.
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.

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.

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] National Vulnerability Database; “CVE-2024-31837 Detail;” https://nvd.nist.gov/vuln/detail/CVE-2024-31837; accessed 30 April 2024

[2] GitHub; “Fix format string and buffer overflow vulnerabilities #12;” https://github.com/jaygreig86/dmitry/pull/12; accessed 30 April 2024

[3] GitHub; “Stack-based buffer overflow in DMitry (Deepmagic…;” https://github.com/advisories/GHSA-494m-pv6g-vh73; accessed 30 April 2024

CAL-CSIC-202404-011

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.

TLP:CLEAR

2