National Cyber Security Centre

2309280140-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

WebP Vulnerability CVE-2023-4863

Thursday 28th September, 2023

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Researchers have discovered a flaw within the libwebp image library which may write data out of bounds to the heap. The libwebp library, which is responsible for encoding and decoding webp images, is present in a variety of software across mobile and desktop platforms. The vulnerability has been assigned CVE-2023-4863 with a CVSS 3.0 score of 8.8. Exploitation occurs when a victim opens a maliciously crafted image, leading to arbitrary code execution and sensitive user data access.

Products Affected

WebP is used by many applications and operating systems. Any application or operating system that uses the libWebP library version up to 1.3.1 is affected by this vulnerability. This may include custom applications.

Products affected include but are not limited to:

- Major web browsers (Firefox, Edge, Chrome)
- Electron based applications
- Flutter based applications
- Linux based operating systems such as Debian, Fedora, OpenSUSE

Impact

Exploitation of CVE-2023-4863 could allow an attacker to perform an out of bounds memory write, achieving code execution on the target system. Google is aware of this vulnerability being exploited in the wild.

Recommendations

The NCSC strongly advises affected organisations to identify any applications that are using libWebP and update accordingly. The NCSC advises that organisations apply mitigations per vendor instructions or discontinue use of the products if mitigations or updates are unavailable. Applications which perform updates automatically may have already updated to a non-vulnerable release.

Further information is available on the NIST website at the link below: `https://nvd.nist.gov/vuln/detail/CVE-2023-4863`

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie