NCSC
National Cyber Security Centre

2103261013-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Critical Vulnerabilities in OpenSSL (CVE-2021-3450, CVE-2021-3449)

2021-03-26

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, 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.*

Threat Type	NCSC has been made aware of two critical vulnerabilities affecting OpenSSL that require **immediate patching where possible**. CVE-2021-3450 affects the certificate chain and CVE-2021-3449 may result in a Denial of Service attack. Please review the OpenSSL advisory here. • **CVE-2021-3450:** The X509_V_FLAG_X509_STRICT flag enables additional security checks of the certificates present in a certificate chain. It is not set by default. Starting from OpenSSL version 1.1.1h a check to disallow certificates in the chain that have explicitly encoded elliptic curve parameters was added as an additional strict check. An error in the implementation of this check meant that the result of a previous check to confirm that certificates in the chain are valid CA certificates was overwritten. This effectively bypasses the check that non-CA certificates must not be able to issue other certificates. If a "purpose" has been configured then there is a subsequent opportunity for checks that the certificate is a valid CA. All of the named "purpose" values implemented in libcrypto perform this check. Therefore, where a purpose is set the certificate chain will still be rejected even when the strict flag has been used. A purpose is set by default in libssl client and server certificate verification routines, but it can be overridden or removed by an application. In order to be affected, an application must explicitly set the X509_V_FLAG_X509_STRICT verification flag and either not set a purpose for the certificate verification or, in the case of TLS client or server applications, override the default purpose. • **CVE-2021-3449:** The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources.

Products Affected	• **CVE-2021-3450** – OpenSSL versions 1.1.1h and newer are affected by this issue (**Note:** OpenSSL 1.0.2 is not impacted by this issue.) • **CVE-2021-3449** – All OpenSSL 1.1.1 versions are affected by this issue. (**Note:** OpenSSL 1.0.2 is not impacted by this issue.)
Impact	• **CVE-2021-3450:** Can lead to a malicious certificate being incorrectly accepted by a server or client. • **CVE-2021-3449:** Denial of Service.
Recommendations	• **CVE-2021-3450:** Users of OpenSSL verisons 1.1.1h and newer should upgrade to OpenSSL 1.1.1k. • **CVE-2021-3449:** All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. (**Note:** OpenSSL 1.0.2 is not impacted by this issue).

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