

CVE Report #11010 - CVE-2026-35189 Linux confirmed

Personen

Zugewiesen an	CVE Review	Verantwortlich
---------------	------------	----------------

CVE Details

CveID	CVE-2026-35189	Device category	Linux
Software component	openssl	Assessment	user mitigation
Version Fixed			

Details

Priorität	Normal	Datum	08.10.2026 -
Kategorie		Version	

Beschreibung

CVE-2026-35189

NVDS

<https://nvd.nist.gov/vuln/detail/CVE-2026-35189>

Component

openssl 3.5.8

Score

V2=0.0 V3=5.3 V4=0.0

Vector

NETWORK

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Description

Issue summary: A certificate with many nameRelativeToCRLIssuer CRL distribution points causes disproportionate heap growth when OpenSSL caches X.509 extensions.

Impact summary: Receiving a crafted certificate from a malicious peer can lead to significant memory pressure and possible Denial of Service in clients or in servers that solicit client certificates.

CWE: CWE-770: Allocation of Resources Without Limits or Throttling

Description: A certificate or a set of certificates that fits under the limit for size of certificates accepted from the peer (~100 KiB) can result in allocation of several hundred MiB of resident memory on the receiving side during a normal TLS handshake. This may be enough to crash the client or server, if multiple concurrent connections lead to similarly large memory allocations.

The fix postpones processing of the CRL distribution points extensions in certificates to the time when the processed value is required for CRL processing. This avoids keeping large memory allocations for a long time when such certificates are received.

FIPS impact: no

The affected code is outside the FIPS module boundary.

Advisory

Until a patch is made available, users that secure Modbus, MbusSlave or Transparent TCP Servers with client certificates should disable the services or implement additional security measures (e.g. a firewall) to prevent unauthorized use.

The configuration parameters for the certificate authentication are MODBUS_CA_FILE, MBUS_TRANSPARENT_CA_FILE, WMBUS_TRANSPARENT_CA_FILE, DLDERS_TRANSPARENT_CA_FILE, MBUSSLVMETER_CA_FILE, MBUSSLV2METER_CA_FILE.

Risk

If TCP Servers of the MUC application are configured to require TLS client certificate authentication, an attacker could cause memory exhaustion by sending specially-crafted certificates without any prior authentication or correctly signed certificates. The memory exhaustion will lead to a kill and restart of the MUC application and cause service outages (DoS).

The usage of client authentication for the server ports is a very uncommon configuration and requires setting parameters directly in the chip.ini.