Cente Technical Information

発行番号	011-0002	Rev	第1版	発行日	2020/08/31
題名	SSL/TLS証明書の検証に失敗することがある				
情報分類	障害情報				
適用製品	・Cente Compact Crypto Ver 1.00-1.22 このモジュールを含み、影響を受けるパッケージは以下の通りです。 ・Cente Compact SSLc Ver 1.00-1.51 ※以下のパッケージはこのモジュールを含みますが、該当機能は使用しないため、影響ありません。 ・Cente Compact SSLd Ver 1.00				
関連資料	なし				

【該当するユーザ環境】
以下の2つの条件を両方満たす環境。
- SSL/TLS証明書(以下単に「証明書」とします)の検証機能を有効にする。
- 証明書のsignatureまたはissuerに、1つのOIDに複数の型が存在する。

また、以下のパッケージで、Cente Compact SSLcを組み合わせて暗号通信し、上記条件を満たす場合も該当します。
- Cente Compact DTLSc(Compact SSLオプション)。
- Cente TCP/IPv4のFTPc。
- Cente HTTPd/cのHTTPc。
- Cente SMTP/POP。

なお、以下の1つ以上の条件を満たす場合は、問題は発生しません。
- 証明書の検証を無効にする。
- 証明書の1つのOIDに1つの型のみが存在する。

【障害内容、発生理由】
証明書のsignature, issuerは、OIDごとに比較します(住所や名前のような種類ごとに比較します)。比較の際、型(TeletexString, PrintableStringなどがあります)の不一致で、検証エラーとしていました。しかし、あるOIDに複数の型で情報が存在する場合、型の不一致があっても、さらに比較すると、一致する型が存在する可能性がありました。このため、本来は検証でOKとなる証明書を、検証エラーとすることがありました。

例えば、以下の例では問題ありません。OID 2.5.4.11(organizationalUnitName)に複数の情報がありますが、型はPrintableStringのみだからです。
- OID=2.5.4.11, PrintableString: example.com/2048
- OID=2.5.4.11, PrintableString: example ltd.

以下の例では本障害が該当します。TeletexString, PrintableStringの2つの型があるからです。
- OID=2.5.4.11, TeletexString: example.com/2048
- OID=2.5.4.11, PrintableString: example ltd.

【回避方法】
ミドルウェアのソースコードを修正し、正しい検証処理にします。
詳細については、営業担当またはsupport_XXXatmarkXXX_cente.jpまでお問い合わせください(_XXXatmarkXXX_は@にしてください)。

以上