2016 年 12 月 6 日

伊藤忠テクノソリューションズ株式会社

シスコ製品の OpenSSL に関する複数の脆弱性について

シスコ製品に実装されている OpenSSL に関して 6 件の脆弱性が存在する事が判明しました。うち 4 件はメモリリーク、1 件はパディングオラクル攻撃（暗号キーを知らなくても解読可能とする攻撃）、1 件は、EBCDIS システムでの不適切なメモリ処理となっています。リモートの攻撃者が、これらの脆弱性を利用してシステムのクラッシュやサービス拒否（DoS）状態 となる可能性があります。

■脆弱性の詳細情報

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-openssl

発表された脆弱性は、以下 6 種です。

・ASN.1 エンコーダの脆弱性

OpenSSL Untrusted ASN.1 Structures Out-of-Bounds Write Vulnerability

OpenSSL d2i_CMS_bio Function Denial of Service Vulnerability

・不十分なパディングをチェックによる脆弱性

OpenSSL AES CBC Cipher Man-in-the-Middle Vulnerability

・EVP_EncodeUpdate()関数の処理の問題による脆弱性

OpenSSL EVP_EncryptUpdate Function Overflow Heap Corruption Vulnerability

OpenSSL EVP_EncodeUpdate Function Overflow Vulnerability

・ASN.1 データ処理の脆弱性

OpenSSL d2i_CMS_bio Function Denial of Service Vulnerability

・EBCDIC システムで不適切なメモリプロセスによる脆弱性

OpenSSL ASN.1 Strings X509_NAME_oneline Function Overread Vulnerability

■対象製品

対象製品と該当するバージョンに関しては、下記 URL をご確認ください。

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-openssl

■対処方法

恒久対策として、修正済ソフトウェアへのバージョンアップをお願いします。

■修正ソフトウェアの入手方法

以下のサイトから入手可能です（事前にアカウント登録必要）

http://www.cisco.com/cisco/software/navigator.html

お問い合わせは、弊社担当営業までお願いいたします。

以　上