Lenovo System x/BladeCenter/Flex System/iDataPlex/NeXtScale における CVE-2014-0224 OpenSSL CCSインジェクションの脆弱性について

当文書は記載時点の情報となります。今後最新の情報に基づき追加・変更されます。

OpenSSLに関する脆弱性が報告されています。この脆弱性はCVE-2014-0224として識別されているもので、「CCSインジェクションに関する脆弱性」とも呼ばれます。
2014年4月に報告された、OpenSSL Heartbleed脆弱性（CVE-2014-0160)とは異なる脆弱性です。

（参考）IPA 「OpenSSL」における Change Cipher Spec メッセージ処理の脆弱性対策について（JVN#61247051）

以下のバージョンが対象となります。

サーバー側：
OpenSSL 1.0.1系統のうち、1.0.1gおよびそれ以前

クライアント側：
OpenSSL 1.0.1 系列のうち 1.0.1g およびそれ以前
OpenSSL 1.0.0 系列のうち 1.0.0l およびそれ以前
OpenSSL 0.9.8 系列のうち 0.9.8y およびそれ以前

Lenovoハードウェア製品・ソフトウェア製品およびIBMソフトウェア製品に関して、影響および対応は以下のサイトにて逐次更新されます。
IBM Product Security Incident Response

System x/BladeCenter/Flex System/iDataPlex/NeXtScale/PureFlex/Flex Systemの各製品におけるCVE-2014-0224 OpenSSL脆弱性の影響および対応方法は以下のとおりです。
利便性向上のために下表にまとめていますが更新の時間差がある場合がありますので、最新状況についてはIBM Product Security Incident Responseも参照してください。

1.該当する製品
（一部調査中の製品を含みます）

サーバー製品

製品名称	該当するコンポーネント	該当バージョン	修正済みバージョン	対応手順
BladeCenter				
BladeCenter S(8886) BladeCenter E(8677) BladeCenter H(8852) BladeCenter HT(8740/8750)	AMM	v3.66E (BPET66E, BBET66E, BPEO66E) およびそれ以前のバージョン	v3.66F (BBET66F)	修正バージョンのファームウェアを適用（以下参照） Security Bulletin: IBM BladeCenter Advanced Management Module is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298, and CVE-2014-3470.
BladeCenter Virtual Fabric 10 Gb Ethernet Switch Module		ファームウェア・バージョン 7.7.4.0以前	7.7.4.0	修正バージョンのファームウェアを適用（以下参照） Security Bulletin: IBM System Networking switches that are affected by the OpenSSL vulnerability: CVE-2014-0224
BladeCenter 1/10Gb Uplink Ethernet Switch Module		ファームウェア・バージョン 7.4.7.0以前	7.7.4.0	
iDataPlex				
NeXtScale nx360 M2	IMM	v1.42およびそれ以前	v1.44, YUOOG6C	修正バージョンのファームウェアを適用（以下参照） Security Bulletin: IBM System x Integrated Management Module (IMM) is affected by the following OpenSSL vulnerabilities:
NeXtScale nx360 M3				

				CVE-2014-0224, CVE-2014-0076
System x iDataplex dx360 M4 System x iDataplex dx360 M4 Xeon E5-2600 v2搭載モデル	IMM2		v4.31, 1AOO58T	修正バージョンのファームウェアを適用
NeXtScale				
NeXtScale nx360 M4	IMM2		v3.91, 1AOO56P	修正バージョンのファームウェアを適用
System x(M2世代)				
System x3400 M2	IMM	v1.42およびそれ以前	v1.44, YUOOG6C	修正バージョンのファームウェアを適用（以下参照） Security Bulletin: IBM System x Integrated Management Module (IMM) is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0076
System x3500 M2				
System x3550 M2				
System x3650 M2				
System x(M3/X5世代)				
System x3200 M3	IMM	v1.42およびそれ以前	v1.44, YUOOG6C	修正バージョンのファームウェアを適用（以下参照） Security Bulletin: IBM System x Integrated Management Module (IMM) is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0076
System x3250 M3				
System x3400 M3				
System x3500 M3				
System x3550 M3				
System x3620 M3				
System x3630 M3				
System x3650 M3				
System x3690 X5		v1.43およびそれ以前		
System x3850/x3950 X5				
System x (M4/X6世代)				

System x3100 M4	IMM2		v4.31, 1AOO58T	修正バージョンのファームウェアを適用
System x3250 M4				
System x3250 M5				
System x3300 M4				
System x3500 M4 System x3500 M4 Xeon E5-2600 v2搭載モデル				
System x3530 M4 System x3530 M4 Xeon E5-2400 v2搭載モデル				
System x3550 M4 System x3550 M4 Xeon E5-2600 v2搭載モデル				
System x3630 M4 System x3630 M4 Xeon E5-2400 v2搭載モデル				
System x3650 M4 System x3650 M4 Xeon E5-2600 v2搭載モデル				
System x3650 M4 HD				
System x3650 M4 BD				
System x3750 M4				
System x3850 X6			v4.02, 1AOO58S	修正バージョンのファームウェアを適用
PureFlex/Flex System				
Flex System	CMM	2.0.0K(2PEO12K)およびそれ以前	v2.0.0, (2PET12N)	修正バージョンのファームウェアを適用 (以下参照) Security Bulletin: IBM Flex System Chassis Management Module

				(CMM) is affected by the following OpenSSL vulnerability: CVE-2014-0224
Flex System x222 Flex System x240 Flex System x440 Flex System x280 Flex System x480 Flex System x880	IMM2	1.34(1AOO28Q) – 4.20(1AOO58R)	v4.21, 1AOO58U	修正バージョンのファームウェアを適用（以下参照） Security Bulletin: IBM Flex System Integrated Management Module II (IMM2) is affected by the following OpenSSL vulnerability: CVE-2014-0224
Flex System Manager Node		確認中	fsmfix1.3.1.0_IT02336	修正済みバージョンを使用
Flex System Fabric EN4093/EN4093R 10Gb Scalable Switch Flex System Fabric CN4093 10Gb Converged Scalable Switch Flex System Fabric SI4093 System Interconnect Module Flex System EN2092 1Gb Ethernet Scalable Switch		ファームウェア・バージョン 7.8.4.0 およびそれ以前	7.8.5.0	修正バージョンのファームウェアを適用（以下参照） Security Bulletin: IBM System Networking switches that are affected by the OpenSSL vulnerability: CVE-2014-0224
Flex System V7000		コードリリース 6.4.1.10以前 7.1.0.10以前 7.2.0.7以前	コードリリース 7.1.0.10以上 7.2.0.7以上	修正バージョンのファームウェアを適用（以下参照） Security Bulletin: OpenSSL vulnerability in IBM Flex System V7000 (CVE-2014-0224)

ネットワーク製品(TOR)

製品名称	該当バージョン	修正済みバージョン	対応手順
System Networking RackSwitch G8264CS	ファームウェア・バージョン 7.8.4.0およびそれ以前	7.8.5.0	修正バージョンのファームウェアを適用 (以下参照) Security Bulletin: IBM System Networking switches that are affected by the OpenSSL vulnerability: CVE-2014-0224
Flex System Interconnect Fabric	ファームウェア・バージョン 7.8.4.0		
Rackswitch G8052 Rackswitch G8124 Rackswitch G8124-E Rackswitch G8124-ER	ファームウェア・バージョン 7.7.10.0以前	7.7.10.0	
RackSwitch G8264 RackSwitch G8264-T RackSwitch G8316			
RackSwitch G8332	ファームウェア・バージョン 7.7.16.0以前	7.7.16.0	

管理ツール類

製品名称	該当バージョン	修正済みバージョン	対応手順
MegCLI	8.05.06 and earlier levels	3Qリリース予定	以下のいずれかの対応を実施 1.StorCLIを使用する 2.ローカルでのみ使用する 3. 修正済みバージョンを使用する(3Q リリース予定) (以下参照) MegaRAID Storage Manager and MegaCLI OpenSSL vulnerabilities discovered - IBM Systems
MSM(MegaRAID Storage Manager)		3Qリリース予定	

ToolsCenterツール類

製品名称	該当バージョン	修正済みバージョン	対応手順
ToolsCenter Suite	Version 9.52およびそれ以前	Version 9.53	修正済みバージョンを使用（以下参照） Security Bulletin: IBM ToolsCenter (including ToolsCenter Suite, ASU, DSA, and USXPi) is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298, CVE-2014-3470
ASU (Advanced Settings Utility)	Version 9.60およびそれ以前	Version 9.61	
UpdateXpress	Version 9.60およびそれ以前	Version 9.61	
DSA (Dynamic System Analysis)	Version 9.60およびそれ以前	Version 9.61	
BoMC (Bootable Media Creator)	確認中		
FastSetup	Version 3.11およびそれ以前	Version 3.2	修正済みバージョンを使用（以下参照） Security Bulletin: IBM FastSetup is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298, CVE-2014-3470

ソフトウェア製品

製品名称	該当バージョン	修正済みバージョン	対応手順
SmarterCloud Entry	3.2	以下のFixにより修正 SmartCloud Entry 3.2.0.2 Hyper-V Agent iFix SmartCloud Entry 3.2.0.2 Appliance iFix	修正バージョンのFixを適用（以下参照） Security Bulletin: SmartCloud Entry is affected by the following OpenSSL vulnerabilities: (List CVEs applicable to your product could include CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298, CVE-2014-3470 and possibly CVE-2014-0
IBM Cloud Manager with OpenStack	4.1	以下のFixにより修正 IBM Cloud Manager with OpenStack 4.1.0.1 iFix IBM Cloud Manager with OpenStack self-service portal 4.1.0.1 iFix	修正バージョンのFixを適用（以下参照） Security Bulletin: IBM Cloud Manager with OpenStack is affected by the following OpenSSL vulnerabilities: (List CVEs applicable to your product could include CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298, CVE-2014-3470 and pos
SmartCloud Provisioning	2.3 and 2.3 FP1	"Enablement Bundle for Virtual Applications and System Plugins on Windows" バンドルを削除するのみ	（以下参照） Security Bulletin: SmartCloud Provisioning is affected by the following OpenSSL vulnerabilities (CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198,

			CVE-2010-5298, CVE-2014-3470, CVE-2014-0076)
IBM SDN VE	確認中		
IBM Systems Director	確認中		
Upward Integration for VMware vSphere	Version 3.0.2 およびそれ以前	IBM Upward Integration Modules (UIM) for VMware vSphere, version 3.5	修正バージョンのFixを適用（以下参照） Security Bulletin: IBM Upward Integration Modules (UIM) is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298, CVE-2014-3470
Upward Integration for Microsoft System Center	Version 5.0.2 およびそれ以前 UIM Hardware Management Pack 5.0.1 and 5.0 UIM Deployment Pack 5.0.2 and earlier UIM System Updates 5.0.2 and earlier UIM Inventory Tool 5.0.2 and earlier UIM Integrated Installer 5.0.2 and earlier	IBM Upward Integration Modules (UIM) for Microsoft System Center, version 5.5, including the following components: UIM Hardware Management Pack 5.5 UIM Deployment Pack 5.5 UIM System Updates 5.5 UIM Inventory Tool 5.5 UIM Integrated Installer 5.5	修正バージョンのFixを適用（以下参照） Security Bulletin: IBM Upward Integration Modules (UIM) is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298, CVE-2014-3470

参考情報

IBM ストレージ製品

IBM SAN Volume Controller
IBM Storwize V7000
IBM Storwize V5000
IBM Storwize V3700
IBM Storwize V3500
Security Bulletin: OpenSSL vulnerability in IBM SAN Volume Controller and Storwize Family (CVE-2014-0224)

IBM XIV Gen3
Security Bulletin: IBM XIV Gen3 Storage System is exposed to the following OpenSSL vulnerability: CVE-2014-0224

TS3400
Security Bulletin: TS3400 is affected by the following OpenSSL vulnerabilities: CVE-2014-0224

IBM ソフトウェア製品

GPFS
Security Bulletin: GPFS V3.5 for Windows is affected by the following OpenSSL vulnerabilities: CVE-2014-0224

VMware
VMware assessment of OpenSSL security vulnerabilities disclosed June 5, 2014 (CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298, CVE-2014-3470) (2079783)

Impact of OpenSSL Security Advisories CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298, and CVE-2014-3470 on VMware Customer Portals and web sites (2079789)

VMware ESXi 5.5, Patch ESXi-5.5.0-20140604001-standard (2077361)

RedHat
OpenSSL CCS インジェクションの脆弱性（CVE-2014-0224）の警告

Novell
CVE-2014-0224

OpenSSL Man in the Middle CVE-2014-0224 CVE-2014-0221 CVE-2014-3470

Juniper products
2014-06 Out of Cycle Security Bulletin: Vulnerabilities in OpenSSL related to ChangeCipherSpec, DTLS, SSL_MODE_RELEASE_BUFFERS and ECDH ciphersuites

Junos Pulse/SA (SSLVPN): Details on fixes for SSL/TLS MITM vulnerability (CVE-2014-0224)/JSA10629

更新履歴

2014/07/08　公開
2014/07/19　MegaCLI、MSM追記