Lenovo System x/BladeCenter/Flex System/iDataPlex/NeXtScale における CVE-2014-0160 OpenSSL Heartbleed 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-2014-0160として識別されているもので、以下のバージョンが対象となります。

OpenSSL 1.0.1 から 1.0.1f

OpenSSL 1.0.2-beta から 1.0.2-beta1

（参考）IPA OpenSSL の脆弱性対策について(CVE-2014-0160)

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集約されており逐次更新されます。

IBM Product Security Incident Response

OpenSSL Heartbleed (CVE-2014-0160)

System x/BladeCenter/Flex System/iDataPlex/NeXtScaleの各製品における CVE-2014-0160 OpenSSL Heartbleed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	v3.66B (BPET66B) v3.66B (BBET66B) v3.66B (BPEO66B) v3.66C (BPET66C) v3.66C (BBET66C) v3.66C (BPEO66C)	Version 3.66d, BPET66D	1.修正バージョンのファームウェアを適用 2.SSL Certificatesの更新 3.User Credentialsのリセット （以下参照） セキュリティー報告：BladeCenter Advanced Management Module(AMM)へのOpenSSL脆弱性による影響 (CVE-2014-0160 and CVE-2014-0076)
iDataPlex				
System x iDataplex dx360 M4 System x iDataplex dx360 M4　Xeon E5-2600 v2搭載モデル	IMM2	v3.81 (1AOO52Z) v3.80 (1AOO52U) v3.76 (1AOO52S) v3.74 (1AOO52R) v3.71 (1AOO52W) v3.70 (1AOO52Q) v3.67 (1AOO50G) v3.65 (1AOO50D)	Version 3.73, 1AOO56D	1.修正バージョンのファームウェアを適用 2.SSL Certificatesの更新 3.User Credentialsのリセット （以下参照） セキュリティー報告：System x Integrated Management Module2(IMM2)へのOpenSSL脆弱性による影響 (CVE-2014-0160 and CVE-2014-0076)

		v3.40 (1AOO48M) v3.37 (1AOO48P) v3.36 (1AOO48Q) v3.35 (1AOO48N) v3.30 (1AOO48L) v3.37 (1AOO48P) v3.10 (1AOO48H) v2.52 (1AOO42E) v2.50 (1AOO40Z)		
NeXtScale				
NeXtScale nx360 M4	IMM2	v3.81 (1AOO52Z) v3.80 (1AOO52U) v3.76 (1AOO52S) v3.74 (1AOO52R) v3.71 (1AOO52W) v3.70 (1AOO52Q) v3.67 (1AOO50G) v3.65 (1AOO50D)	Version 3.83, 1AOO56I	1.修正バージョンのファームウェアを適用 2.SSL Certificatesの更新 3.User Credentialsのリセット （以下参照） セキュリティー報告：System x Integrated Management Module2(IMM2)へのOpenSSL脆弱性による影響 (CVE-2014-0160 and CVE-2014-0076)

		v3.40 (1AOO48M) v3.37 (1AOO48P) v3.36 (1AOO48Q) v3.35 (1AOO48N) v3.30 (1AOO48L) v3.37 (1AOO48P) v3.10 (1AOO48H) v2.52 (1AOO42E) v2.50 (1AOO40Z)		
System x				
System x3100 M4	IMM2	v3.81 (1AOO52Z) v3.80 (1AOO52U) v3.76 (1AOO52S) v3.74 (1AOO52R) v3.71 (1AOO52W) v3.70 (1AOO52Q) v3.67 (1AOO50G) v3.65	Version 3.73, 1AOO56D	1.修正バージョンのファームウェアを適用 2.SSL Certificatesの更新 3.User Credentialsのリセット （以下参照） セキュリティー報告：System x Integrated Management Module2(IMM2)へのOpenSSL脆弱性による影響 (CVE-2014-0160 and CVE-2014-0076)
System x3250 M4			Version 3.73, 1AOO56D	
System x3250 M5			Version 3.83, 1AOO56I	
System x3300 M4			Version 3.84, 1AOO56J	
System x3500 M4 System x3500 M4 Xeon E5-2600 v2搭			Version 3.73, 1AOO56D	

載モデル		(1AOO50D) v3.40 (1AOO48M) v3.37 (1AOO48P) v3.36 (1AOO48Q) v3.35 (1AOO48N) v3.30 (1AOO48L) v3.37 (1AOO48P) v3.10 (1AOO48H) v2.52 (1AOO42E) v2.50 (1AOO40Z)		
System x3530 M4 System x3530 M4 Xeon E5-2400 v2搭載モデル			Version 3.77, 1AOO56H	
System x3550 M4 System x3550 M4 Xeon E5-2600 v2搭載モデル			Version 3.73, 1AOO56D	
System x3630 M4 System x3630 M4 Xeon E5-2400 v2搭載モデル			Version 3.77, 1AOO56H	
System x3650 M4 System x3650 M4 Xeon E5-2600 v2搭載モデル			Version 3.73, 1AOO56D	
System x3650 M4 HD			Version 3.86, 1AOO56L	
System x3650 M4 BD			Version 3.75, 1AOO56F	
System x3750 M4			Version 3.73, 1AOO56D	
System x3850 X6			Version 3.82, 1AOO56E	
PureFlex/Flex System				
PureFlex/Flex System製品については以下の情報をご参照ください。 PureFlexにおけるCVE-2014-0160 OpenSSL Heartbleed脆弱性の影響				

(14_001_TFL_PUREFLEX)

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	修正済みバージョンを使用 https://www-947.ibm.com/support/entry/myportal/docdisplay?lndocid=TOOL-TCSUITE
ASU (Advanced Settings Utility)		Version 9.52, Build ID: ASUT83A	修正済みバージョンを使用 https://www-947.ibm.com/support/entry/myportal/docdisplay?lndocid=TOOL-ASU
UpdateXpress		Version 9.52	修正済みバージョンを使用 https://www-947.ibm.com/support/entry/myportal/docdisplay?lndocid=SERV-XPRESS
DSA (Dynamic System Analysis)		Version 9.52, Build ID DSYTBD3L	修正済みバージョンを使用 https://www-947.ibm.com/support/entry/myportal/docdisplay?lndocid=SERV-DSA
BoMC (Bootable Media Creator)		Version 9.52	修正済みバージョンを使用 https://www-947.ibm.com/support/entry/myportal/docdisplay?lndocid=TOOL-BOMC

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	3.1 (Hyper-V Agent Installerを使用している場合) 3.2 (アプライアンスもしくはHyper-V Agent Installerを使用している場合)	3.1.0.3 Hyper-V Agent iFix (2014年4月16日リリース済) 3.2.0.2 Appliance iFix (2014年4月15日リリース済) 3.2.0.2 Hyper-V Agent iFix (2014年4月16日リリース済)	1.修正バージョンのFixを適用 2.SSL Certificatesの更新 3.User Credentialsのリセット (以下参照) Security Bulletin: SmartCloud Entry is affected by vulnerabilities in OpenSSL (CVE-2014-0160 and CVE-2014-0076)
IBM SDN VE	IBM SDN VE, Unified Controller, VMware Edition: 1.0.0 IBM SDN VE, Unified Controller, KVM Edition: 1.0.0 IBM SDN VE, Unified Controller, OpenFlow Edition: 1.0.0 IBM SDN VE,	IBM SDN VE, Unified Controller, VMware Edition: version 1.0.1 or later IBM SDN VE, Unified Controller, KVM Edition: version 1.0.1 or later IBM SDN VE, Unified Controller, OpenFlow Edition: version 1.0.1 or later	1.修正バージョンのFixを適用 2.SSL Certificatesの更新 3.User Credentialsのリセット (以下参照) Security Bulletin: IBM SDN for Virtual Environments is affected by a vulnerability in OpenSSL

	Dove Management Console, VMware Edition: 1.0.0		(CVE-2014-0160)
IBM Systems Director	IBM Systems Director: 6.3.2.0, 6.3.2.1, 6.3.3.0. 6.3.3.1	SysDir6_3_x_0_IT01062_IT01063_IT01199	1.修正バージョンのFixを適用 2.SSL Certificatesの更新 3.User Credentialsのリセット （以下参照） IBM Systems Directorが持つOpenSSL脆弱性への対応について (CVE-2014-0160 および CVE-2014-0076)
Flex System Manager	<Flex System Manager> Flex System Manager 1.3.1 <管理エージェント> IBM Systems Director	<Flex System Manager> Flex System Manager 1.3.1.1(FSMApplianceFixPackage-1-3-1-1) <管理エージェント> Flex System 1.3.1 Platform Agents(Flex1_3_1_Platform_Agents_IT00284)	1.修正バージョンのFixを適用 2.SSL Certificatesの更新 3.User Credentialsのリセット 4.パスワードの変更 （以下参照） Security Bulletin: Flex System

	Platform Agent for Windows 6.3.4 IBM Systems Director Common Agent for Windows 6.3.4 IBM Systems Director Platform Agent for Linux 6.3.4 IBM Systems Director Common Agent for Linux 6.3.4		Manager (FSM) and compatible IBM Systems Director agents are affected by vulnerabilities in OpenSSL (CVE-2014-0160 and CVE-2014-0076)
Upward Integration for VMware vSphere	IBM Upward Integration Modules (UIM) for VMware vSphere, version 3.0.1 and earlier	IBM Upward Integration Modules (UIM) for VMware vSphere, version 3.0.2	1.修正バージョンのFixを適用 2.SSL Certificatesの更新 3.User Credentialsのリセット （以下参照） Security Bulletin: IBM Upward Integration

			Modules (UIM) is affected by vulnerabilities in OpenSSL (CVE-2014-0160 and CVE-2014-0076)
Upward Integration for Microsoft System Center	IBM Upward Integration Modules (UIM) for Microsoft System Center, version 5.0.1 and earlier, including the following components: UIM Deployment Pack 5.0.1 and earlier UIM System Updates 5.0.1 and earlier UIM Inventory Tool 5.0.1 and earlier UIM Configuration Pack 5.0.1	IBM Upward Integration Modules (UIM) for Microsoft System Center, version 5.0.2, including the following components: UIM Deployment Pack 5.0.2 UIM System Updates 5.0.2 UIM Inventory Tool 5.0.2 UIM Configuration Pack 5.0.2 UIM Integrated Installer 5.0.2	1.修正バージョンのFixを適用 2.SSL Certificatesの更新 3.User Credentialsのリセット （以下参照） Security Bulletin: IBM Upward Integration Modules (UIM) is affected by vulnerabilities in OpenSSL (CVE-2014-0160 and CVE-2014-0076)

	and earlier UIM Integrated Installer 5.0.1 and earlier		

(参考)ストレージ製品

IBMストレージ製品におけるOpenSSLの脆弱性について(14_001_TFL_STOR)
http://www-01.ibm.com/support/docview.wss?uid=jpn1J1011679

2.該当しない製品

サーバー製品

IBM System x products not affected by the OpenSSL Heartbleed vulnerability (CVE-2014-0160) Flash (Alert)

ネットワーク製品

CVE-2014-0160 Security Classification, Tip 29911

ソフトウェア製品

IBM Fabric Manager

(参考)ストレージ製品

IBMストレージ製品におけるOpenSSLの脆弱性について(14_001_TFL_STOR)
http://www-01.ibm.com/support/docview.wss?uid=jpn1J1011679

参考情報

VMware
VMware Security Advisories
VMSA-2014-0004.2
VMware product updates address OpenSSL security vulnerabilities

RedHat

OpenSSL の CVE-2014-0160 (Heartbleed バグ) と Red Hat Enterprise Linux

Novell

CVE-2014-0160 Common Vulnerabilities and Exposures

Microsoft

Microsoft サービスは OpenSSL「Heartbleed」脆弱性の影響を受けません

Juniper products

2014-04 Out of Cycle Security Bulletin: Multiple products affected by OpenSSL "Heartbleed" issue (CVE-2014-0160)

Brocade products

BROCADE TECHNICAL SUPPORT BULLETIN TSB 2014-185A [2]

更新履歴

2014/04/22　公開

2014/04/23　ストレージ製品に関する参考情報の追記およびJuniper社、Brocade社の参考情報の追記

2014/04/25　PureFlex/Flex Systemに関する情報公開先へのリンクを追記

2014/05/01　AMMおよびIMM2の対応手順について、日本語版のガイドへのURLリンクに更新、ISD、FSM、UIM(VMware,Microsoft)の記載を追記、ToolsCenterの記載を追記

2014/05/12　IBM Systems Directorの対応手順について、日本語版のガイドのURLリンクに更新