Yokogawa Security Advisory Report

YSAR-18-0002

公開日 2018-04-05
最終更新日 2018-04-05

YSAR-18-0002: PC セットにリモート管理機能のアクセス制限不備の脆弱性 2

概要:

一部の PC セットに搭載されたリモート管理機能に、アクセス制御不備の脆弱性が存在することを確認しました。以下に、この脆弱性の影響を受ける製品をご案内いたします。
本レポートの内容をご確認の上、影響を受ける製品を含むシステム全体のセキュリティ対策などを総合的にご判断いただき、必要に応じて対策の適用をご検討ください。

影響を受ける製品:

下記製品は、影響を受ける可能性があります。
お使いの製品が該当するかどうかは、「対策方法」に記載の方法で確認してください。

No	製品分類	機種	基本形名	用途	対象
1	PC セット	Dell Precision T3600	R/DLHIS3600	HIS 用	国内
2			R/EXAPC3600	EXA 用	
3			R/WGDLHIS3600	WEBFREX 用	
4			R/BMDLHIS3600	BM 用	
5			R/DELLT3600	交換専用	
6			R/DLHIS3600B	VP BASIC 用	
7			R/DLHIS3600E	HIS 間接輸出	海外 （間接輸出）

脆弱性詳細:

Intel 社が提供するリモート管理機能に、アクセス制限不備の脆弱性が存在することが公開されました。
リモート管理機能である Intel® Active Management Technology(AMT)が有効になっている場合、リモートから管理機能の権限を奪われる恐れがあります。

CVSS v2 における本脆弱性の基本値は 9.0、現状値は 7.4 です。

攻撃元区分(AV)	ローカル(L)		隣接(A)		ネットワーク(N)
攻撃条件の複雑さ(AC)	高(H)		中(M)		低(L)
攻撃前の認証要否(Au)	複数(M)		単一(S)		不要(N)
機密性への影響(C)	なし(N)		部分的(P)		全面的(C)
完全性への影響(I)	なし(N)		部分的(P)		全面的(C)
可用性への影響(A)	なし(N)		部分的(P)		全面的(C)

攻撃される可能性(E)	未実証(U)	実証可能(POC)	攻撃可能(F)	容易に攻撃可能(H)	未評価(ND)
利用可能な対策レベル(RL)	正式(OF)	暫定(TF)	非公式(W)	なし(U)	未評価(ND)
脆弱性情報の信頼性(RC)	未確認(UC)	未確証(UR)	確認済(C)	未評価(ND)	

対策方法:

BIOS の設定画面より AMT が有効となっているか確認してください。
有効となっている場合は本脆弱性の影響を受ける為、無効に変更してください。(*1)(*2)(*3)(*4)

※詳細は後述の「脆弱性の影響を受ける製品と対策方法」をご確認ください。

*1：Dell 社から、本脆弱性の対策版 BIOS がリリースされていますが、PC セットでは使用できません。AMT を無効にしてお使いください。
*2：AMT の確認および変更には PC の再起動が必要となります。
*3：マザーボード上の電池を交換した場合、設定内容は消去されます。再設定を行ってください。
*4：YSAR-17-0001 で公開された脆弱性対策を実施済みの場合、この対策は必要ありません。

脆弱性の影響を受ける製品と対策方法:

機種	対策方法
Dell Precision T3600	(1) BIOS 設定画面の呼び出し 1.1 PC を再起動します。 1.2 BIOS 初期起動画面（Dell のロゴ画面）が表示されたら、直ちに<Ctrl>+<P>キーを押します。 1.3 <Ctrl>+<P>キーの入力を受け付けると、設定画面 “Intel® Management Engine BIOS Extension” が呼び出されます。 (2) ユーザ認証 2.1 設定画面を呼び出した後、パスワードを入力します。初期パスワードは “admin” です。 2.2 設定画面を初めて呼び出した場合は、初期パスワード入力後、パスワードの変更を求められます。 ※変更後のパスワードはお客様にて適切に管理してください。 (3) AMT の無効化 3.1 設定画面より “Intel® AMT Configuration” を選択して<Enter>キーを押します。 3.2 “Manageability Feature Selection” を選択して<Enter>キーを押します。 3.3 確認画面が表示されますので、<Y>キーを押します。 “Enable” の場合は本脆弱性の影響を受ける為、3.4 の手順を実施してください。 3.4 “Disable”を選択して<Enter>キーを押します。 (4) 設定の終了 4.1 “Previous Menu” を選択して<Enter>キーを押します。 4.2 “Exit” を選択して<Enter>キーを押します。 4.3 確認画面が表示されますので、<Y>キーを押します。 4.4 PC が自動的に再起動します。

なお、今回確認された脆弱性に限らず、システム全体において適切なセキュリティ対策を講じていただくことを推奨しています。

お問い合わせ先:

本レポートの内容に関するご質問等については、下記にお問い合わせください。
https://contact.yokogawa.com/cs/gw?c-id=000523

参考:

1. CVSS（共通脆弱性評価システム）について
   http://www.ipa.go.jp/security/vuln/CVSS.html
   共通脆弱性評価システム CVSS （ Common Vulnerability Scoring System）は、情報システムの脆弱性に対するベンダーに依存しない汎用的な評価手法です。脆弱性の深刻度を同一の基準の下で定量的に比較でき

るようになります。
本レポートに記載されている CVSS の各値は現状のまま提供するものであり、いかなる保証も伴いません。
本レポートに記載されている脆弱性が実際にどれだけの深刻度があるかについては、影響を受ける製品を含むシステム全体のセキュリティ対策などを総合的に判断した上で、お客様自身で評価していただく必要があります。

2. JVN の脆弱性レポート：JVNDB-2017-010467, JVNDB-2017-010525, JVNDB-2017-010519, JVNDB-2017-010520, JVNDB-2017-010521, JVNDB-2017-010522, JVNDB-2017-010523, JVNDB-2017-010524
   https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-010467.html
   https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-010525.html
   https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-010519.html
   https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-010520.html
   https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-010521.html
   https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-010522.html
   https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-010523.html
   https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-010524.html

更新履歴:

2018-04-05: 初版

※本レポートの内容については、将来予告なしに変更することがあります。