

Press Release
報道関係者各位

平成 24 年 9 月 4 日
株式会社ユビテック
(JASDAQ コード: 6662)

「Ubiteq Android アプリケーション脆弱性検証サービス」をサービスイン ～Android 実装アプリケーションを対象としたセキュリティ脆弱性の診断サービス～

ユビキタスプラットフォーム事業の創生を目指す株式会社ユビテック（東京都品川区、代表取締役社長：荻野司、以下「ユビテック」）は、Android 実装アプリケーションを対象とした「Ubiteq Android アプリケーション脆弱性検証サービス」を 2012 年 9 月より開始いたしました。

■マルウェア・ウイルスアプリの危険性

近年市場で増大し続けているマルウェア（※）やウイルスアプリによる被害は、実に 7 割が非常にベーシックな Android 仕様の理解不足から発生しております。お客様が開発された大切な Android 実装アプリケーションが悪意ある第三者のアプリに悪用される事を事前防止するために、「Ubiteq Android アプリケーション脆弱性検証サービス」を是非お役立ててください。

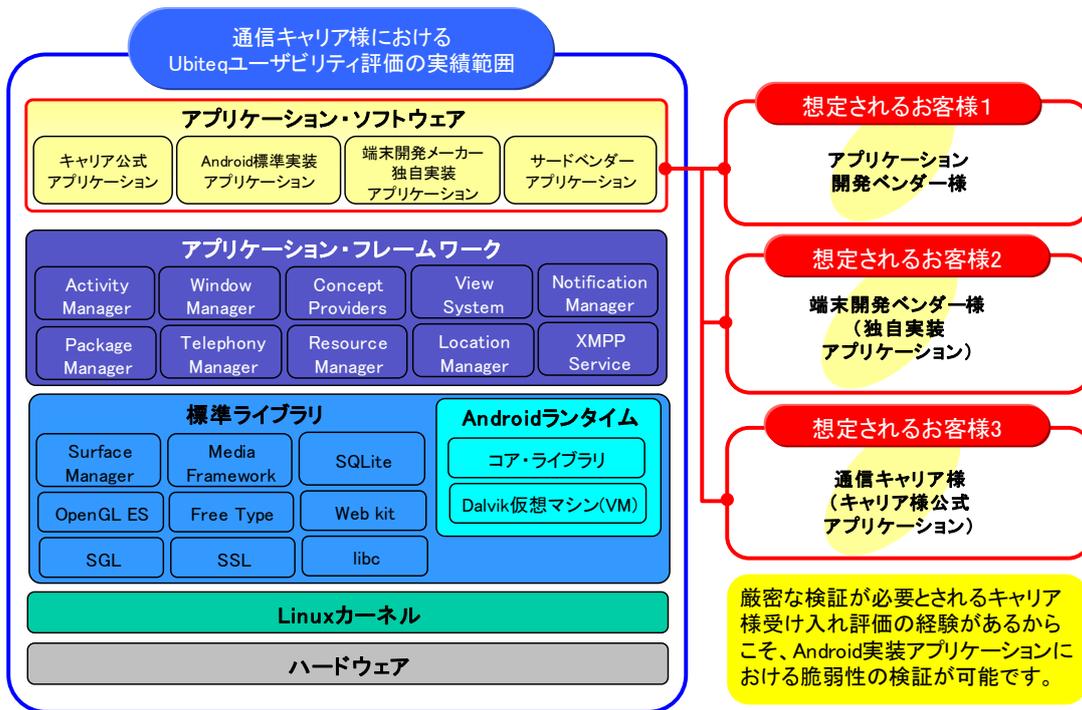
※:マルウェア (Malware)

不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称のことです。日本では「悪意のあるソフトウェア」または「不正プログラム」とも呼ばれています。

■「Ubiteq Android アプリケーション脆弱性検証サービス」のメリット

- 15 年に渡る通信キャリア受け入れ評価によって培われた確かな評価品質。
- お客様のご予算、必要性にあわせて、3つのレベルから対象範囲を自由に選択可能。
- セキュリティリスクが分かりやすい図解入りで示された脆弱性診断レポート。
- リスク回避の方法についても具体的にご説明いたします。

■「Ubiteq Android 実装アプリケーション脆弱性検証サービス」の検証対象 ～ お客様イメージ



■ Ubiteq Android 実装アプリケーション脆弱性検証サービスの概要

検証メニューは、基本的なセキュリティ対策の有無を検証するレベル1から、高度なセキュリティ対策の有無を検証するレベル3までをご用意しております。各レベルを組み合わせる事で、お客様のご予算と必要性に応じて、柔軟な検証が可能です。

※各検証レベルはそれぞれ個別にご契約いただけます。

	検証レベル	検証メニュー	回避可能な脆弱性事例
基本的な セキュリティ対策 ↓ より高度な セキュリティ対策	[レベル1] アプリケーションの 悪用防止	Androidパーミッションの検証	・攻撃アプリケーションから勝手に、課金番号へ電話発信される ・個人情報を勝手にサーバに送信される …etc.
		独自定義パーミッションの検証	
		…etc.	
	[レベル2] データ保護	データ格納ディレクトリの妥当性検証	・格納データが不正に利用される/外部へ流出する ・ソースコードをコピーされ不正に転売される ・一部を書き換えられたマルウェアとして転用される …etc.
		ファイルパーミッションの検証	
		独自定義ディレクトリの検証(暗号化)	
		ソースコードの難読化 …etc.	
	[レベル3] 情報不正傍受 ・盗み見防止	インテント エキストラパラメータの検証	・アプリケーション間の処理から「個人情報」や「機密情報」を盗み見される …etc.
…etc.			

■ 実際のマーケットアプリケーションにおける脆弱性診断レポートサンプル

脆弱性に関する詳細説明

①「android.intent.action.CALL_PRIVILEGED」の定義に関する脆弱性

【脆弱性の影響】 **—セキュリティリスクレベル:S(非常に危険)—**

適切なパーミッションを持たない任意のアプリケーションからCALL_PRIVILEGEDアクション(緊急通話を含む通話呼び出し)を受け付けてしまう。このため、CALL_PHONEパーミッション(電話発信許可)を持たないアプリケーションが対象アプリケーションを通じて電話発信が出来てしまう。

電話発信

対象アプリケーション
CALL_PHONE (電話発信) パーミッション

悪意あるアプリケーション
CALL_PHONE (電話発信) パーミッション

CALL_PRIVILEGED +81XXXXXXXXXX

制限をかけていないため、任意のアプリケーションから上記Intentを受信してしまう

CALL_PRIVILEGEDパーミッションを持たない悪意あるアプリからのIntent受信によって、対象アプリケーションから「+81XXXXXXXXXX」に電話発信されてしまう可能性がある

独自基準によるリスクレベル表示

図解による分かりやすい想定リスク説明

リスク回避方法を具体的に示唆

【セキュリティ向上のための対策】

対象アプリケーションのIntent定義で、相手にCALL_PHONEパーミッションを要求するように定義することで上記の脆弱性を回避できる。

■現状の定義
<activity android:enabled="true" ……>

■脆弱性を回避するための定義例
<activity android:enabled="true" permission="android.permission.CALL_PRIVILEGED" ……>

引き続きユビテックでは、お客様製品の品質向上に最大限貢献するため、効果的かつ効率的な検証サービスの提供に取り組んでまいります。

【本件に関するお問い合わせ先】

株式会社ユビテック 担当：管理本部 総務課

電話：03-5487-5560 FAX：03-5487-5561