JSSEC 技術部会

脆弱性WG 年間活動報告

脆弱性WGの取組み成果と今後の展開について

2012年5月

1. 脆弱性WGの活動概要

1. スマートフォン全般における「脆弱性情報」を収集・分析し、脆弱性のチェックリストを作成してJSSEC内で情報シェアを実施。

2. 外部向けへの公開(データベース化も含めて)については、IPAの脆弱性対策情報データベース(JVN)と作業が被るため、JSSEC参加の各企業からIPAに直接報告し、JVNのデータベースに情報を集約。

3. JSSECに参画しているデバイスメーカー様向けに、安全なドライバー作成方法等の講義及び意見交換を実施。

2. 脆弱性に対するアプローチ

■現状課題
キャリア及びデバイスメーカーにとって脆弱性対策は、クリティカルな問題が発生して表面化しないかぎり、人・コスト・時間を掛けられる余裕がないのが現状。
打開策として、以下のように脆弱性対策のレイヤを切り分けて整理した。

①チップセット共通の脆弱性
脆弱性WGとして調査・分析を継続し、IPA/JP-CERT様を介して、Googleや海外のチップベンダーに働きかける。

②組み込みドライバー等の脆弱性
デバイスメーカーが独自に組み込んでいるドライバーの脆弱性は、クリティカルな問題に発展する可能性は低いので、修正が完了した時点で、各メーカー様からIPA/JP-CERTに自主的に報告。

③影響度の高い脆弱性
マルウェアへの転用など、影響度の高い脆弱性については、今後も脆弱性WGとして調査・分析を継続し、状況に応じてマルウェアWGと連携予定。

3. 脆弱性の一例

■Linuxカーネルの脆弱性
JSSEC参加企業で対策情報の共有化を実施
→マルウェアへの転用は現状なし。

■Androidブラウザ関連の脆弱性
IPAに報告済み(Googleさん他)
対象Android2.1～全部のようだ
製品により修正状況は異なる(非公開)
→マルウェアへの転用は現状なし。

■Android 4.x(ICS)の脆弱性
IPAに2件報告(Googleさん他)
CVE番号が振られましたが、まだ非公開
最新版のICSにはまだ未適用
→マルウェアへの転用は現状なし。

3. 安全な端末の作り方講座の報告①

- シャープ、富士通さんのところに行き、安全な端末の作り方講座を開催
- 通端末独自の脆弱性のデモを交えました
- 2011/12/15 シャープさん
- 2011/3/27 富士通東芝モバイルさん
- 良かった点
  - おおむね好印象で講演が行えた
  - 百名ぐらいの方に聞いていただけた（大石さんに感謝）
  - 現場の作り手の方の考えが聞けたこと
  - セキュアコーディングの大事さ、ほんのちょっとの穴がroot奪取につながる点を認識してもらえた
  - 外部との交流がプラスになるという意見が聞けた
  - 問題形式で脆弱性発見について参加者に解答してもらえたことで、参加意識が高められたと思う。

3. 安全な端末の作り方講座の報告②

- 残念だった点
  - Javaを書いている人たちが多数参加していただいていたのに、Java関連まで話が出来なかった。(時間不足、メンバー不足)
  - 脆弱性のほかに、マルウェア関連の話も出来ればよかった
- 今回は脆弱性を利用する人がどのように端末の穴を探すのか、という攻撃側の攻撃手順と、脆弱性のあるドライバをどのように見つけるかが中心
- ドライバの開発が中心になったため、ミドルウェアやJava層のセキュリティの話は出来なかった
- 今後も内容をブラッシュアップ、対応範囲もミドルウェア、Java層、アプリケーション含めて講義できるようにしたい

3. 安全な端末の作り方講座～今後の予定

- パナソニックさんで、講義予定
- ソニーさん
- シャープさん、第2弾を予定
- NEC（座談会？）

今後も要望があれば相談に乗りますので、気軽にお声掛けください。

Thank You !