先週公開の「Java 7」パッチは不完全、脆弱性が残る――研究者が指摘

「オラクルが修正し残した脆弱性によりJavaサンドボックスを回避可能」と報告

(2012年09月03日)

「Java 7」に発見された深刻な脆弱性を修正する目的で、先週、米国Oracleが公開したアップデートに対して、ポーランドのセキュリティ研究者が「新たな脆弱性を発見した」と指摘している。

30日に公開されたJava 7 Update 7のリリース・ノートでは、具体的な修正内容には触れられていなかった

ポーランドに本拠を置くSecurity Explorationsの設立者でCEO(最高経営責任者)を務めるアダム・ゴーディアック(Adam Gowdiak)氏は、IDGの取材に対し、「この新たな脆弱性に関する報告と概念実証コードを、8月31日付でOracleに送付した」と語った。また、新たな脆弱性の技術的詳細は、Oracleによる修正作業が完了するまでは公表しないとしている。

8月30日、Oracleは4カ月ごとの通常リリース・サイクルを外れた緊急アップデートとして「Java 7 Update 7」をリリースした。同アップデートで修正対象となった3件の脆弱性のうち2件は、攻撃者がJavaサンドボックスを回避して任意のOSコードを実行できるという深刻なものだ。

さらに、残る1件の脆弱性は「潜在的なセキュリティ問題」とされる。Oracleによれば、この脆弱性を直接攻撃に使うことはできないが、そのほかの脆弱性の影響をさらに悪化させるために使われるおそれがあるという。

ゴーディアック氏が「攻撃ベクター(exploitation vector)」と呼ぶこの「潜在的なセキュリティ問題」を修正することで、すでにSecurity ExplorationsからOracleに報告済みの、Javaサンドボックスを回避する概念実証コードはすべて無効(実行不可能)になった。

ゴーディアック氏によると、Security Explorationsでは今年4月、Oracleに対し、今回修正された2件も含む29件の脆弱性を内密に報告していた。この報告では、脆弱性の情報だけでなく16件の概念実証コードも提供された。

「sun.awt.SunToolkitクラスの実装からgetFieldメソッドとgetMethodメソッドが削除されたことで、Java 7 Update 7ではSecurity Explorationsが提供した概念実証コードがすべて無効になった」(ゴーディアック氏)

しかしながらゴーディアック氏は、概念実証コードは「攻撃ベクター」が削除されたために無効になっただけであり、攻撃者がターゲットにしうるすべての脆弱性が修正されたわけではない、と指摘する。

「アップデート(Java 7 Update 7)の適用によって(同社が提供した)概念実証コードが機能しなくなったことを確認したのち、当社では再び概念実証コードを見直し、アップデート後の最新版Javaでセキュリティを突破できる方法がないかを検証した」(ゴーディアック氏)

Security ExplorationsがJava 7 Update 7に発見した新たな脆弱性は、Oracleが修正し残した幾つかの脆弱性が組み合わさることで、再びJavaサンドボックスを回避可能になってしまうものだという。

この新たな脆弱性をOracleがいつ修正するつもりなのか、ゴーディアック氏にはわからないという。通常のリリース・サイクルである10月のセキュリティ・アップデートで修正されるかどうかも不明瞭だ。Oracleからのコメントは得られなかった。

ゴーディアック氏も、多くのセキュリティ研究者たちがこれまで呼びかけてきた警告を繰り返している。「Javaを使う必要がないならば、システムからアンインストールすべきだ」。

(Lucian Constantin／IDG News Serviceルーマニア支局)