平成 27 年3月 16 日

Topic

Elasticsearch の脆弱性を標的としたアクセスの観測について

オープンソースの全文検索システム Elasticsearch に、リモートから任意のコマンドが実行できる脆弱性が存在することが公表され、警察庁の定点観測でも当該脆弱性を標的としたアクセスを観測しました。Elasticsearch のバージョンアップや設定変更等のセキュリティ対策を実施することを推奨します。

1 Elasticsearch の脆弱性を標的としたアクセスの観測

2月中旬、オープンソースの全文検索システム Elasticsearch に、リモートから任意のコマンドが実行できる脆弱性が存在することが公表されました[i]。3月には、当該脆弱性を検証するためのプログラム(PoC[ii])が公開されていることを確認しており、警察庁の定点観測システムにおいても、当該脆弱性を標的としたと思われるアクセスを観測しています(図)。

これらのアクセスは、脆弱性のある Elasticsearch が稼動しているかどうかの探索を行っていると考えられるものの他、実際に PoC 等を利用して、任意のコマンドの実行を試みているものが観測されました。また、実行を試みたコマンドとしては、OS 情報の取得や外部サーバからの不審なファイルのダウンロード等が確認されました。不審なファイルについては、指令サーバからの要求に応じて、DoS 攻撃等を行うボットプログラムとして利用されるものであると考えられます。

なお、3月 10 日に観測されたアクセスのほとんどは、特定の IP アドレスからのもので、OS 情報の取得を試みているものでした。

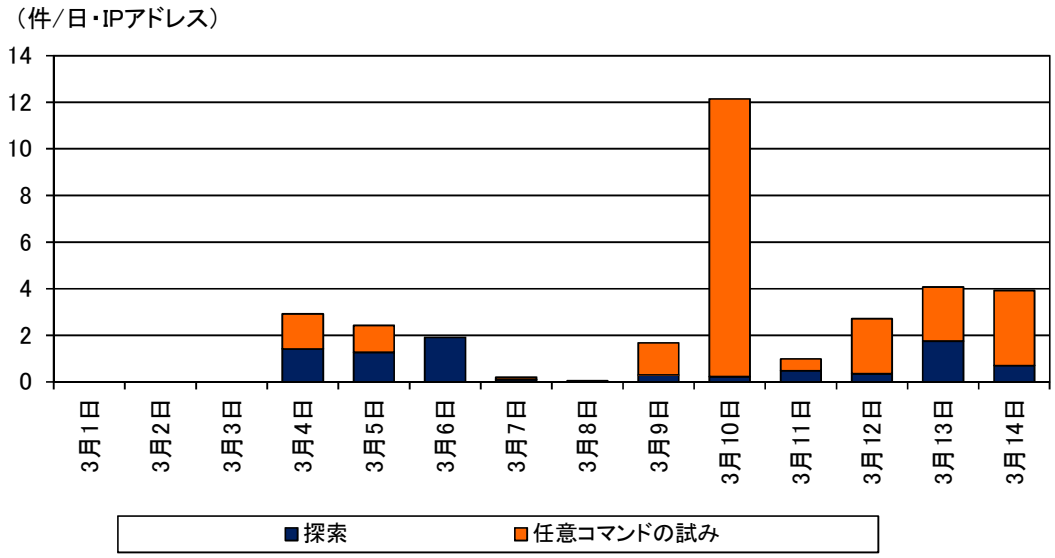

図 Elasticsearch の脆弱性を標的としたと思われるアクセスの推移(3月1日～14 日)

i 「Elasticsearch の Groovy スクリプトエンジンにおけるサンドボックス保護メカニズムを回避される脆弱性」
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001538.html
ii Proof of Concept の略。脆弱性を利用した攻撃が可能であることを示すための検証用プログラムのこと。

2 推奨する対策

Elasticsearch を使用している場合は、ベンダからの情報[i]を参考にして、バージョンアップや設定の変更等を行うことを推奨します。また、不審なファイルが存在しないか、不正なアクセスが行われていないかなどの確認を行うことも大切です。

i https://www.elastic.co/blog/elasticsearch-1-4-3-and-1-3-8-released