セキュリティ総論 D レポート No.6

慶應義塾大学 理工学部物理学科 61908697 佐々木良輔

Shellshock とは

Shellshock (CVE-2014-6271, CVE-2014-7169) は GNU Bash <= 4.3 に存在する脆弱性である．これは以下のような環境変数による関数定義においてパーサーのバグによって関数定義の後に書かれた任意のコードが実行されるという脆弱性である.[1]

Listing 1　攻撃コード例

```
1 env CVE_2014_6271="(){echo␣'Hello';};␣echo␣'Goodbye'" bash -c CVE_2014_6271
```

上記のコードにおいて期待される動作は Hello が出力されることであるが, 脆弱なシステムでは Goodbye が同様に出力される．このようなワンライナーを用いることで任意のコードが実行される可能性がある．Bash は多くの Linux ディストリビューションで標準のシェルとして用いられているため, 脆弱性の影響は非常に広範囲に及んだ.

対応の例

脆弱性はシステムに対するパッチの適用や Bash のアップデートで解決された．システムベンダーやホスティングサービス事業者などは利用者の脆弱性が存在する製品のリスト (またはシステムの脆弱性の判定方法) や脆弱性がある場合の対処方法を公開しており, システム運用者はその情報を元に脆弱性の解決を行う必要がある.[2][3][4][5]

広範囲に及ぶ脆弱性に対する対応

Shellshock では脆弱性に対する対応としてベンダーなどは対処方法の周知を行い, その情報を元に各運用者が対処を行った.

このように広範囲に影響が及ぶ脆弱性の場合は, ベンダーや政府機関による情報の周知と, それに応じた運用者の行動が対処として現実的であると考えられる．情報の公開について, 広範囲に情報を公開することは攻撃者にとっても攻撃を容易にするが, ゼロデイ攻撃を防ぐためには早期に多くの利用者に情報を伝える必要がある．したがって利用者は脆弱性の発見後直ぐに攻撃の有無の確認や更新プログラム適用の準備を行い, またサービスのプロバイダはできるだけ早く更新プログラムを作成する必要があると考えられる.

参考文献

[1] Alex Blewitt. Shellshock の衝撃. https://www.infoq.com/jp/news/2014/10/shellshock1/, 9 2014. (Accessed on 01/12/2022).

[2] さくらインターネット. あなたのサーバは大丈夫？ shellshock 対策をしましょう. https://knowledge.sakura.ad.jp/2580/, 10 2014. (Accessed on 01/12/2022).

[3] HITACHI. 日立製品における gnu bash の脆弱性 (cve-2014-6271、cve-2014-7169 他) への対応について. https://www.hitachi.co.jp/hirt/publications/hirt-pub14011/index.html, 1 2015. (Accessed on 01/12/2022).

[4] Red Hat Customer Portal. Cve-2014-7169. https://access.redhat.com/security/cve/cve-2014-7169, 9 2014. (Accessed on 01/12/2022).

[5] 情報処理推進機構. bash の脆弱性対策について. https://www.ipa.go.jp/security/ciadr/vul/20140926-bash.html, 10 2014. (Accessed on 01/12/2022).