CloudCoffer

2020 年 9 月 30 日

セキュリティニュース：

Web メールの新たな脅威を発見

今回は、脆弱性情報もあまねく行き渡って使われているハズなのに見落とされていた、複数の要素の技術を組み合わせた脆弱性を突く攻撃 が捉えられたのでそれを紹介する。

CloudCoffer のシステムは、URI 内に HTTP referer、セッション ID などの情報が含まれているかも確認しています。今回はそのロジックでアラート条件に掛かりました。

リスク度合い：

Critical（CVSS スコア:10.0）

背景：

セッションの識別のために URL 内のセッション ID を使うのはごく普通の利用技術であるが、そのリスクについては、例えば BurpSuite では次の様に紹介されている（英文）。

この、ID の一般的な仕組みは qiita.com の説明が分かり易い。

例として、次の Web メールサーバを考える。 https://webmail.company.com.
ユーザ A は、この Web メールへのログインの後、例えば、自動生成された次の URL を使うようになる。

https://webmail.company.com/?sessionID=dk31kc1jgkkvva31

ここで、"dk31kc1jgkkvva31" はユーザ A の今回のログインに指定されたセッション ID である。ただし、ユーザがこれを明示指定する訳ではないし、URL 表示にも出てこないのが普通である（説明例）。

このセッション ID は Web サーバがユーザを識別する用途に使われ、他のユーザや攻撃者には秘密にしておくべき情報である。攻撃者がこのセッション ID を再利用できれば、そのユーザの権限を取得する（そのユーザとしてログインした状態になる）ことができる。

Web メールシステム＋HTML 形式は要注意：

攻撃のシナリオ

攻撃者は HTML 形式なら、"リンク画像" 等の情報をメール内に埋め込むことができる。
それを使って、リモートサーバ（攻撃者の制御下のもの）から動的に画像をダウンロードする「リンク画像」を含むメールを作成、送信する。

ユーザ A がメールを開くと、このリモートサーバに HTTP-GET が送信され、指定画像を取得し表示されるので、**裏で何か他の事が起こっているかもしれない、とはユーザ A は気付かない／疑わない。**

ARIS Advanced Research & Information Service

その際、攻撃者サーバへの HTTP-GET リクエストの中には、「HTTP referer」が ID 値までも含む事になる（これは HTTP プロトコルで規定されている標準の動作）。これで、次の文字列が攻撃者の手許に落ちたことになる（上で想定した、ユーザ A がログインしている状態のセッション ID 情報）。

https://webmail.company.com/?sessionID=dk31kc1jgkkvva31

その後、攻撃者は単純にこの文字列を URL としてコピー＆ペーストで指定してユーザ A として Web メールに接続することができる。
セッションの有効期限が切れていない場合、攻撃者は被害者(すなわちユーザ A)のアカウントをオーナーとして使用することができる。

影響を受けるシステムと対策：

現在、多くの Web メールシステムが影響を受ける状況にある。

- Open Webmail 系のシステムは特に注意されたい（おそらく最初に発見されていて該当システム数が多い）。
- 新しいパッチが適用されるまでは、HTML 形式メールの場合は、内容を直接表示しないようにすることをお勧めする。一度、平文テキストとして保存し、単機能のメモ帳などで表示すれば、外部リンクへの接続リスクは大幅に軽減される。
- （見知らぬユーザからのメール等は特に）画像等の添付がある場合は、これらを無条件にクリックしないようにもするべき。

昨今は、HTTP ヘッダ部の機能を使った攻撃が増え高度化しているのに、シグネチャに頼る WAF 製品によっては、HTTP ヘッダ部分の確認すらしないものも有ります。HTTP ボディ部分の確認をするものはさらに少数なので、そのように対策が不十分なサイトではユーザの操作をマニュアル制限するなどの人間系の努力も必須です。ただし、各自に覚えて置いてもらって回避するしか無いので、十分に徹底することは望み薄ではある。

お問い合わせ先：株式会社アリス　AI セキュリティ事業部 <aisec@aris-kk.co.jp>
CCC（CloudCoffer on Cloud）サイト：https://ccc.cloudcoffer.jp
CloudCoffer サイト：https://www.cloudcoffer.jp
RayAegis Japan サイト：https://www.rayaegis.co.jp

以上、少しでもご参考になれば幸いです。