

Privileges Escalation(特権昇格)

Privileges Escalation (特権昇格)とは

例えば、一般ユーザとしてログインしているユーザが、システムや管理者権限でしか使用できないコマンドを使用するなど、持っている権限以上の権限でしか許可されていないコマンドや機能を使用できようになることをPrivileges Escalation(特権昇格)という。

Privileges Escalation(特権昇格)の概念は、攻撃手法そのものというより、攻撃の目的/弱点をついた結果であると言えるが、管理者権限で動くサービスやプロセスの弱点について暴走させ、任意のコマンドを実行するといったパターンが多い。

手法解説

Privileges Escalation を引き起こすために、下記のような手法(パターン)が考えられる。

- UNIX上で、SUID/SGIDプログラムがBuffer Overflow や Format String などの弱点を持っている場合に、それらの弱点についてプログラムを暴走させ、任意のコマンドを実行する
- OSのセキュリティ管理の設計ミスで、一般ユーザからのリクエストを、システム権限で起動するプロセスが受け付ける

関連項目

Buffer Overflow , Format String

影響

管理者権限やシステム権限を奪われることによって、攻撃対象マシンのあらゆる制御が可能になる。結果としてやサービス不能による業務の停滞や機密情報の漏洩、社会的信用の失墜などの致命的な損害を被る可能性がある。

影響を受けるOS、サービス

OS・サービス	バージョン	備考
全般		

OS、サービス、アプリケーション 全般
バージョン

対策方法

ホストの要塞化の上、関連するVulnerability ごとの対策を施す