Linuxカーネル == セキュリティの悪夢

Marcel Holtmann
Red Hat Security Response Team
PacSec 2006 Conference: Tokyo, Japan

この条件式は

- 真
  - 起きててくださいね
  - 深刻な問題はすでに発生しているので、なんとかしなければいけない
- 偽
  - 寝ないでくださいね
  - この先も悪夢にしてしまわないように

議題

- Linuxカーネルのセキュリティ対応について
- Insights to our processes
- 配布元とディストリビューション/ベンダーの違い
- 過去6ヶ月における脆弱性の詳細な考察
- システムをセキュアにするテクノロジー

セキュリティ対応

- セキュリティ問題に迅速に対応
- 想定される影響を調査
- 影響を受けるバージョンを特定
- CVE名を割り当て
- 各ベンダーと協議
- 機密維持
- アップデートのリリース

情報源

- vendor-sec@lst.de
  - 各ベンダーのセキュリティ専門家によるクローズドなグループ
  - Linux (Unix) 関係が中心
  - 招待制
- security@kernel.org
  - 約6名からなるLinuxカーネルコミュニティの小規模なグループ
- Full disclosure and Bugtraq
  - 公開メーリングリスト

セキュリティレベル

- Red Hatはマイクロソフトと同じ区分手法を採用

深刻度の詳細

- 緊急(Critical)
  - 悪用されるとユーザの介入なしにインターネットワームが拡散するおそれがある脆弱性
- 重要(Important)
  - 機密性、完全性、可用性のいずれかが容易に侵害される
- 警告(Moderate)
  - 悪用が困難もしくはその可能性が低い
- 注意(Low)
  - 悪用が非常に困難もしくはその影響がごくわずか

影響を受けるカーネル

- 配布元のカーネル
  - メインラインの2.4および2.6カーネル
  - 安定版のブランチ
- ディストリビューションのカーネル
  - 配布元のカーネルから枝分かれ
  - パッチと新機能のバックポート
  - Red Hat Enterprise Linux 2.1のカーネルは2.4.9ベース(2001年8月16日リリース)

CVE名

- Common Vulnerabilities and Exposures
- 「脆弱性および情報セキュリティ障害を標準化した名称の一覧 － CVEの目的は既知の脆弱性および情報セキュリティ障害の完全な標準化である」
- http://cve.mitre.org/
- 例: CVE-2006-2451

機密保持

- 立場によって意見は異なる
  - 意見を持つのは自由
- 機密保持にはSensible use of embargoes
- リスクの期間を最小限に抑えるのに必要
- 顧客とオープンソースコミュニティのバランス
- 一般的な機密保持期間は1、2週間
- リリースは火曜日から木曜日の間
- vendor-secで協議

リリースポリシー

- 緊急(Critical)レベルの脆弱性
  - 機密保持が解禁される、もしくはクオリティエンジニアリングをパスしたらただちにリリース
  - 日時を問わない
- 重要(Important)レベルの脆弱性
  - 充分な期間をあけてリリースすることがある
- 警告、注意レベルの脆弱性
  - 同一のパッケージに他の問題が発見されるまで、もしくは次のアップデートリリースまでリリースを待つことがある

Linuxカーネルのアップデートサイクル

- 通常は3ヶ月ごとに、配布元が新しいバージョンのカーネルをリリース
- 安定版カーネルのリリースは任意だが、セキュリティ上の理由がほとんど
- ディストリビューションが配布するカーネルのセキュリティアップデートは、1ヶ月に1度だけが一般的

脆弱性の分類

- 権限の昇格
  - root権限の奪取
- サービス拒否(ローカルおよびリモート)
  - カーネルパニックやクラッシュ
- 情報漏洩
  - 重要なデータを含むメモリへのアクセス

問題の多い領域

- netfilterのコード
  - ファイアーウォールなどに必要
- 新しいネットワークプロトコル
  - IPv6やSCTPなど
- 普及していないアーキテクチャ
  - CPUにPowerPCやUltraSPARCを使用するマシン
- ファイルシステムの一部

CVE-2006-1864

- SMB共有上のchrootを破る
- smbfsとcifsに影響
- 2.4と2.6カーネルが脆弱
- cifsに関してはバックポートが大変だった
- SMB共有でchrootするのは稀

CVE-2006-2274

- SCTPスタックに対するリモートサービス拒否攻撃
- 無限に再帰処理を実行させ、システムを停止
- 潜在的なSCTPの問題の1つに過ぎない

CVE-2006-0457

- keyringの処理にサービス拒否もしくは情報の漏洩
- 非特権ユーザがカーネルをクラッシュ可能
- 暗号化されたファイルシステムに関する重要な情報を取得可能

CVE-2006-4813

- 情報の漏洩
- __block_prepare_write()関数が使用済メモリのクリアをしない
- root以外は読めないファイルを読み取り可能
- 膨大な情報の漏洩

CVE-2006-3468

- 不正なNFSリクエストによるサービス拒否
- ext3ファイルシステムが停止、read-onlyで再マウント
- 不適切なエラーケースの処理がext3を脆弱に

CVE-2006-2451

- prctl()による権限の昇格
- 基本的に設計上の欠陥
- 機密保持期間は2週間
- DebianとSourceforgeの侵入に使われる
- Red Hatはカーネルのアップデートを公表当日に提供

CVE-2006-3626

- /procによる権限の昇格
- 競合状態と設計上の欠陥
- 金曜の夜に0day exploit
- 配布元は6時間以内に修正
- RHEL4ではSELinuxのデフォルトポリシーが悪用を防ぐ
- 2.4カーネルには影響なし

CVE-2006-3635

- この件は機密保持期間中

問題の概要

- ほとんどの問題はローカルサービス拒否
  - システムにローカルユーザや信頼できないユーザがいない場合は緊急度は低い
- リモートサービス拒否攻撃は実際に起きる
  - ファイアーウォールや他の保護手段がない場合、事態は深刻に
- 権限の昇格/情報の漏洩
  - ローカルユーザや信頼できないユーザがいる場合重大な脅威に

Red Hatのイノベーション

- 攻撃ベクターの削減
  - 2001 ファイアーウォールをデフォルトで有効に
  - 2004 NXおよびソフトウェアNXをデフォルトに
  - 2004 ランダム化
  - 2005 ヒープオーバーフローのチェック
  - 2005 SELinuxをデフォルトで有効に
  - 2006 GlibcとGCCによるチェック
- 常にユーザ空間を管理下に

配布元による努力

- -stableカーネルシリーズを作成
- 2つ前のリリースまでをサポート
- セキュリティ問題の迅速な対応
- すべて問題にCVE名を割り当て
- SuSE/NovelのGreg Kroah-Hartman、Red HatのChris Wrightがメンテナンス

結論

- カーネルのセキュリティは深刻
- 機密保持は慎重に
- 0dayにも迅速に対応
- SELinuxとExec-shieldは有効
- もちろん完璧ではないが、改善の努力は常に継続されている

御静聴ありがとうございました

- Have a good night sleep and dream something nice ...

Linuxカーネル == セキュリティの悪夢

Marcel Holtmann
Red Hat Security Response Team
PacSec 2006 Conference: Tokyo, Japan

この条件式は

- 真
  - 起きててくださいね
  - 深刻な問題はすでに発生しているので、なんとかしなければいけない
- 偽
  - 寝ないでくださいね
  - この先も悪夢にしてしまわないように

議題

- Linuxカーネルのセキュリティ対応について
- Insights to our processes
- 配布元とディストリビューション/ベンダーの違い
- 過去6ヶ月における脆弱性の詳細な考察
- システムをセキュアにするテクノロジー

セキュリティ対応

- セキュリティ問題に迅速に対応
- 想定される影響を調査
- 影響を受けるバージョンを特定
- CVE名を割り当て
- 各ベンダーと協議
- 機密維持
- アップデートのリリース

情報源

- vendor-sec@lst.de
  - 各ベンダーのセキュリティ専門家によるクローズドなグループ
  - Linux (Unix) 関係が中心
  - 招待制
- security@kernel.org
  - 約6名からなるLinuxカーネルコミュニティの小規模なグループ
- Full disclosure and Bugtraq
  - 公開メーリングリスト

セキュリティレベル

- Red Hatはマイクロソフトと同じ区分手法を採用

深刻度の詳細

- 緊急(Critical)
  - 悪用されるとユーザの介入なしにインターネットワームが拡散するおそれがある脆弱性
- 重要(Important)
  - 機密性、完全性、可用性のいずれかが容易に侵害される
- 警告(Moderate)
  - 悪用が困難もしくはその可能性が低い
- 注意(Low)
  - 悪用が非常に困難もしくはその影響がごくわずか

影響を受けるカーネル

- 配布元のカーネル
  - メインラインの2.4および2.6カーネル
  - 安定版のブランチ
- ディストリビューションのカーネル
  - 配布元のカーネルから枝分かれ
  - パッチと新機能のバックポート
  - Red Hat Enterprise Linux 2.1のカーネルは2.4.9ベース(2001年8月16日リリース)

CVE名

- Common Vulnerabilities and Exposures
- 「脆弱性および情報セキュリティ障害を標準化した名称の一覧 – CVEの目的は既知の脆弱性および情報セキュリティ障害の完全な標準化である」
- http://cve.mitre.org/
- 例: CVE-2006-2451

機密保持

- 立場によって意見は異なる
  - 意見を持つのは自由
- 機密保持にはSensible use of embargoes
- リスクの期間を最小限に抑えるのに必要
- 顧客とオープンソースコミュニティのバランス
- 一般的な機密保持期間は1、2週間
- リリースは火曜日から木曜日の間
- vendor-secで協議

リリースポリシー

- 緊急(Critical)レベルの脆弱性
  - 機密保持が解禁される、もしくはクオリティエンジニアリングをパスしたらただちにリリース
  - 日時を問わない
- 重要(Important)レベルの脆弱性
  - 充分な期間をあけてリリースすることがある
- 警告、注意レベルの脆弱性
  - 同一のパッケージに他の問題が発見されるまで、もしくは次のアップデートリリースまでリリースを待つことがある

Linuxカーネルのアップデートサイクル

- 通常は3ヶ月ごとに、配布元が新しいバージョンのカーネルをリリース
- 安定版カーネルのリリースは任意だが、セキュリティ上の理由がほとんど
- ディストリビューションが配布するカーネルのセキュリティアップデートは、1ヶ月に1度だけが一般的

脆弱性の分類

- 権限の昇格
  - root権限の奪取
- サービス拒否(ローカルおよびリモート)
  - カーネルパニックやクラッシュ
- 情報漏洩
  - 重要なデータを含むメモリへのアクセス

問題の多い領域

- netfilterのコード
  - ファイアーウォールなどに必要
- 新しいネットワークプロトコル
  - IPv6やSCTPなど
- 普及していないアーキテクチャ
  - CPUにPowerPCやUltraSPARCを使用するマシン
- ファイルシステムの一部

CVE-2006-1864

- SMB共有上のchrootを破る
- smbfsとcifsに影響
- 2.4と2.6カーネルが脆弱
- cifsに関してはバックポートが大変だった
- SMB共有でchrootするのは稀

CVE-2006-2274

- SCTPスタックに対するリモートサービス拒否攻撃
- 無限に再帰処理を実行させ、システムを停止
- 潜在的なSCTPの問題の1つに過ぎない

CVE-2006-0457

- keyringの処理にサービス拒否もしくは情報の漏洩
- 非特権ユーザがカーネルをクラッシュ可能
- 暗号化されたファイルシステムに関する重要な情報を取得可能

CVE-2006-4813

- 情報の漏洩
- __block_prepare_write()関数が使用済メモリのクリアをしない
- root以外は読めないファイルを読み取り可能
- 膨大な情報の漏洩

CVE-2006-3468

- 不正なNFSリクエストによるサービス拒否
- ext3ファイルシステムが停止、read-onlyで再マウント
- 不適切なエラーケースの処理がext3を脆弱に

CVE-2006-2451

- prctl()による権限の昇格
- 基本的に設計上の欠陥
- 機密保持期間は2週間
- DebianとSourceforgeの侵入に使われる
- Red Hatはカーネルのアップデートを公表当日に提供

CVE-2006-3626

- /procによる権限の昇格
- 競合状態と設計上の欠陥
- 金曜の夜に0day exploit
- 配布元は6時間以内に修正
- RHEL4ではSELinuxのデフォルトポリシーが悪用を防ぐ
- 2.4カーネルには影響なし

CVE-2006-3635

- この件は機密保持期間中

問題の概要

- ほとんどの問題はローカルサービス拒否
  - システムにローカルユーザや信頼できないユーザがいない場合は緊急度は低い
- リモートサービス拒否攻撃は実際に起きる
  - ファイアーウォールや他の保護手段がない場合、事態は深刻に
- 権限の昇格/情報の漏洩
  - ローカルユーザや信頼できないユーザがいる場合重大な脅威に

Red Hatのイノベーション

- 攻撃ベクターの削減
  - 2001 ファイアーウォールをデフォルトで有効に
  - 2004 NXおよびソフトウェアNXをデフォルトに
  - 2004 ランダム化
  - 2005 ヒープオーバーフローのチェック
  - 2005 SELinuxをデフォルトで有効に
  - 2006 GlibcとGCCによるチェック
- 常にユーザ空間を管理下に

配布元による努力

- -stableカーネルシリーズを作成
- 2つ前のリリースまでをサポート
- セキュリティ問題の迅速な対応
- すべて問題にCVE名を割り当て
- SuSE/NovelのGreg Kroah-Hartman、Red HatのChris Wrightがメンテナンス

結論

- カーネルのセキュリティは深刻
- 機密保持は慎重に
- 0dayにも迅速に対応
- SELinuxとExec-shieldは有効
- もちろん完璧ではないが、改善の努力は常に継続されている

御静聴ありがとうございました

- Have a good night sleep and dream something nice ...