Row Hammerの権限昇格の脆弱性

アドバイザリーID : cisco-sa-20150309-rowhammer
初公開日 : 2015-03-09 21:50
最終更新日 : 2016-09-08 19:07
バージョン 1.4 : Final
回避策 : No workarounds available
Cisco バグ ID :

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

2015年3月9日、Double Data Rate Type 3(DDR3)同期ダイナミックランダムアクセスメモリ(SDRAM)の欠陥を利用して、該当ハードウェアを搭載したシステムで権限昇格攻撃を実行する新しい研究が発表されました。欠陥はロウハンマーとして知られています。攻撃を試みるには、攻撃者は該当システムで悪意のあるバイナリを実行する必要があります。

さらに、シスコのサーバクラス製品で使用されているチップセットとメモリモジュールに組み込まれている緩和策やメモリ保護機能が数多くなかったコンシューマハードウェアについても調査の対象となりました。このドキュメントで注目すべきは、研究者がテストでエラー訂正コード(ECC)メモリを使用するデバイスを悪用できなかったことです。

シスコでは、非特権ユーザがバイナリをロードして実行できる製品を限定して提供しています。

この調査レポートは次のリンクにあります。
http://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150309-rowhammer

該当製品

シスコでは、非特権ユーザがバイナリをロードして実行できる製品を限定して提供しています。次のリストの製品は、ユーザーがバイナリを読み込んで実行することを可能にし、現在調査中です。次の各製品には、ECCメモリモジュールなど、Row Hammerイベントに対するハードウェア保護機能が多数搭載されています。最初の調査レポートによると、シスコ製品が影響を受けると考える理由はありません。ただし、シスコでは次の製品に対してテストを行い、確認しています

。

アップデート（2015年3月30日）：シスコデバイスの評価により、ECC DDRAMが搭載され、BIOSでECCチェックオプションが有効になっているデバイスでは、この問題は不正利用できないことが示されています。これは、評価済みのすべての製品のデフォルトの状態です。 すべてのCisco UCSコンピューティングデバイスは、シスコから出荷されたRow Hammerによる権限昇格の攻撃の影響を受けないことが判明しています。 シスコ認定のデュアルインラインメモリモジュールを使用するすべてのCisco UCSデバイスで検証が実施されています。 UCSコンピューティングデバイスにインストールされているDIMMデバイスのうち、シスコ認定部品ではないデバイスが該当する可能性があります。

脆弱性のある製品

Row Hammerによる権限昇格攻撃の影響を受けるシスコ製品は確認されていません。

脆弱性を含んでいないことが確認された製品

この脆弱性を不正利用するには、攻撃者が該当デバイスで任意のコードを実行する必要があります。次のデバイスは、設計によって任意のコードのローカル実行を許可しないことが確認されています。

- Cisco IOSソフトウェアが稼働するデバイス
- Cisco IOS XEソフトウェアを実行するデバイス
- Cisco IOS XRソフトウェアを実行しているデバイス
- Cisco ASAソフトウェアを実行しているデバイス
- Cisco Webセキュリティアプライアンス(WSA)
- Cisco Eメールセキュリティアプライアンス(ESA)
- Cisco NX-OSソフトウェアが稼働するCisco Nexus 2000シリーズデバイス
- Cisco NX-OSソフトウェアを実行しているCisco Nexus 4000シリーズデバイス
- Cisco NX-OSソフトウェアを実行しているCisco Nexus 5000シリーズデバイス
- Cisco NX-OSソフトウェアを実行しているCisco Nexus 6000シリーズデバイス
- Cisco NX-OSソフトウェアが稼働するCisco Nexus 7000シリーズデバイス
- Cisco NX-OSソフトウェアを実行しているCisco MDS 9000シリーズデバイス

次の製品は評価済みで、影響を受けません。

- Cisco NX-OSソフトウェアを実行しているCisco Nexus 3000シリーズデバイス
- Cisco NX-OSソフトウェアを実行しているCisco Nexus 9000シリーズデバイス
- Cisco Unified Computing System Bシリーズブレードサーバ
- Cisco Unified Computing System EシリーズISRブレードサーバ
- Cisco Unified Computing System Cシリーズラックサーバ

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

詳細

Row Hammer DDR3特権昇格の脆弱性

2015年3月9日、DDR3メモリ仕様で発見された既知の問題に関連する新しい調査と調査結果がリリースされました。この新しい研究では、Row Hammerと呼ばれるDDR3メモリの制限クラスを利用しています。Row Hammerの問題は、ハイパフォーマンスコンピューティングがDDR3ベースのシステムに対する要求を高め、障害を引き起こしていた2012年に、業界で初めて大規模に認識されました。当時の一般的な障害事例では、メモリ破損とそれに続くデバイスのクラッシュが発生していました。メモリメーカーとチップセットベンダーの両方が、Row Hammerの対応策を部品に組み込み始めました。

調査レポートは次のとおりです。
http://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html

最新の調査では、これらのタイプのエラーは予測可能な方法で導入できることが示されています。Linuxオペレーティングシステム上で動作するプルーフオブコンセプト(POC)がリリースされました。このプルーフオブコンセプトは、これらのエラーの予測可能性を利用して、権限のないコンテキストから影響を受けるデバイスのメモリを変更します。この機能は、認証されたローカルの攻撃者が攻撃者が提供するバイナリを実行して、攻撃者の権限をスーパーユーザまたはrootアカウントの権限に昇格できる場合に使用されることがあります。

攻撃者はこの問題を引き起こすためにバイナリを実行する必要があるため、非特権ローカルユーザアクセスおよびバイナリを実行する機能を許可するシスコ製品だけが影響を受ける可能性があります。

この調査では、ECCを搭載した製品に対する影響を実証できなかったことが明らかになっています。

回避策

この脆弱性を軽減するための直接的な回避策や修正はありません。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、http://www.cisco.com/go/psirt のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性の不正利用事例とその公表は確認しておりません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150309-rowhammer

改訂履歴

リビジョン 1.4	2015年3月30日	すべてのCisco UCSデバイスが脆弱性を含んでいないことを確認。ドキュメントの状態が最終版に移行しました。
リビジョン 1.3	2015年3月17日	「該当製品」セクションに製品評価ステータスの更新を追加。
リビジョン 1.2	2015年3月11日	製品ステータスを更新。
リビジョン 1.1	2015年3月9日	「エクスプロイトおよび公表」セクションの軽微な変更
リビジョン 1.0	2015年3月9日	初回公開リリース

利用規約

情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。