Cisco OpenDNSパルスDNSサービス拒否攻撃

アドバイザリーID : cisco-sa-opendns-pulse-dos-Dd8L3sZq
初公開日 : 2024-05-20 16:00
最終更新日 : 2024-05-23 16:28
バージョン 1.1 : Final
回避策 : No workarounds available
Cisco バグ ID :

概要

Cisco OpenDNSサービスは、キューに入れられた大量のDNS要求を受信した場合の不適切な処理が原因で、DNSパルス攻撃に対して脆弱でした。この攻撃は、一般的に実装されている複数のDNSメカニズムを利用します。DNSクエリは低レートで送信され、大規模な応答に増幅されます。これにより、DNS応答が短く大量のバーストに集中され、ターゲットシステムが過負荷状態になります。

回避策

この問題に対処する回避策はありません。

修正済みソフトウェア

シスコは、クラウドベースのCisco OpenDNSでこの問題に対処しています。ユーザの対処は必要ありません。サービス GUI のヘルプ機能を使用すると、現在の修復ステータスやソフトウェアバージョンを確認できます。

その他の情報が必要な場合は、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。

不正利用事例と公式発表

Cisco Product Security Incident Response Team(PSIRT)は、このアドバイザリに記載されている攻撃に対して概念実証ガイドラインが利用可能であることを認識しています。

Cisco PSIRTでは、本アドバイザリに記載されている本攻撃の不正利用事例は確認しておりません。

出典

この問題を報告していただいた清華大学NISLラボのShang Li氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-opendns-pulse-dos-Dd8L3sZq

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	脆弱性への参照を削除するように更新。	タイトル、脆弱性ソース	Final	2024年5月23日
1.0	初回公開リリース	—	Final	2024年5月20日

利用規約

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。