

Denial-of-Service Vulnerability in ISC BIND 9

分類 Failure to Handle Exceptional Conditions
 関連ツール名称
 再現性 リモート

技術解説

1) 概要

ISC が開発・配布を行っている DNS サーバである BIND 9 には、特殊なパケットを受信することにより、BIND がシャットダウンする問題がある。なお、これらの問題を利用して、メモリの書換やコード実行は出来ない。

2) 原因

BIND の message.c 中にある dns_message_findtype() 関数において、適切な例外処理をしていないことに原因がある。詳細には、rdataset パラメータに NULL 文字以外が与えられたときの処理を行っていないことが原因である。

影響

DNS サーバである BIND 9 には特殊なパケットを受信することにより、シャットダウンを起こす問題がある。DNS サーバはインターネットの中核を担う存在であり、DNS がサービス不能となることにより、インターネット自体がサービス不能になる可能性がある。

影響を受けるOS、サービス

影響 ○:脆弱性あり、×:脆弱性なし

(2002/6/6現在)

OS	サービス	バージョン	影響	備考
UNIX 全般	BIND	9.2.1	×	このバージョンからは対策済み
		9.2.1 未満	○	
		8.x	×	
		4.x	×	

OS、サービス UNIX 全般
 アプリケーション BIND 9.2.1 未満

対策方法

1) 対策

この問題が対策済みである、BIND 9.2.1 以上にバージョンアップする。または、サービ

スを使用しないのであればサービスを停止する。

最新バージョン入手先 URL:

<http://www.isc.org/products/BIND/bind9.html>

2) Advisory情報

CERT Advisory:

<http://www.cert.org/advisories/CA-2002-15.html>

<http://www.kb.cert.org/vuls/id/739123>

X-Force Advisory:

http://www.iss.net/security_center/alerts/advise119.php

Copyright © 2002 警察庁