TD61-2594C
HCVU000000001
2005年5月25日
日立電線株式会社

ICMPエラーメッセージによるTCPの脆弱性について

1．脆弱性の概要(NISCC-532967)

以下のICMPメッセージを第三者が偽装することにより、TCPが実装された装置のコネクションを強制的に終了させる、通信速度を低下させるなどのサービス運用妨害(Denial of Service)攻撃の可能性が報告されています(JPCERT/CC REPORT 2005-04-20)。

・TCPコネクション強制終了を誘発する可能性があるICMP(hard error)メッセージ:

(1) Destination Unreachable

- Protocol Unreachable (type 3, code 2)
- Port Unreachable (type 3, code 3)
- Fragment Needed and Don't Fragment was set (type 3, code 4)

・TCP通信のスループット低下を誘発する可能性があるICMPメッセージ:

(2) Destination Unreachable(PMTUD)

- Fragment Needed and Don't Fragment was set (type 3, code 4)

(3) Source Quench (type 4)

2．参考情報

(1) JP Vendor Status Notes NISCC-532967
TCP 実装の ICMP エラーメッセージの処理に関する脆弱性
http://jvn.jp/niscc/532967/

(2) US-CERT/CC VU#222750

3．当社製品への影響

当社製品の本脆弱性に関する影響は下記の通りです。

製品名	OS名称	影響
Apresia®8000シリーズ	ApWare	本脆弱性に該当しません
Apresia®6000シリーズ	ApbWare	
Apresia®4000シリーズ	AEOS®	
Apresia®3000シリーズ	AEOS®, HSWWare Ver3,5	
Apresia®2000シリーズ	AEOS®, HSWWare Ver2,4	
GMXシリーズ	GMX-Ware1 GMX-Ware3 GMX-Ware4	
HSWシリーズ	HSWWare Ver2 HSWWare Ver3	現在まで本脆弱性に関する影響は見つかっておりません。継続して調査中です。

以上