Security Bulletin SB003

Severity: Medium

Teradici Zero Client firmware 5.5.2

Summary

This security bulletin describes a security vulnerability that has been resolved in Teradici Zero Client firmware 5.5.2. Full details of affected products are listed in ***Table 1***.

Affects all Teradici Zero Client firmware 4.x and 5.x older than 5.5.2

This vulnerability could allow a remote attacker to arbitrarily modify host timestamp values, leading to a denial-of-service condition (VU#637934).

Severity

This security bulletin is rated Medium severity.

Definitions for severity levels are on page 3.

Risks

If this fix is not applied, a remote attacker could cause a denial of service condition resulting in the data flow between Zero Client and Host to stop.

Resolution

Forward this bulletin to your site security controller, administrators or managers of the Amulet Hotkey zero client models listed in ***Table 1***.

Update all Zero Clients to Teradici firmware 5.5.2

Important Note: Teradici firmware 5.5.2 can only be managed by PCoIP Management Console 2.0 or higher.

More information

If you need any further details or clarification about this Security Bulletin, please contact your Amulet Hotkey account manager or support team:

UK +44 (0)20 7960 2400

US +1 (212) 269 9600

Europe eurosupport@amulethotkey.com

US ussupport@amulethotkey.com

Asia apsupport@amulethotkey.com

Affected Products

Zero Client Model	Part Number
DXZ4-A	CA-DXZ4-A001
DXZ4-AM	CA-DXZ4-AM01
DXZC-A	CA-DXZC-3003
DXZC-AM	CA-DXZC-3M03
DXZC-AC	CA-DXZC-3C02
DXZC-AMC	CA-DXZC-3MC1
DXZC-AE	CA-DXZC-4011
DXZC-AEM	CA-DXZC-4M11
DXZC-AEC	CA-DXZC-4021
DXZC-AEMC	CA-DXZC-4M21

Table 1: List of affected Zero Clients

Severity definitions

High (Critical)

- For any failure of the product to comply with its security objectives and security requirements that constitutes an exploitable vulnerability and results in a security breach.
- The associated attack is usually easily/commonly available and can be completed by an unauthenticated attacker; and the result is usually a compromise of root or Administrator; or arbitrary code execution.

Medium (Major)

- For any inability to comply with assurance requirements which increases the risk of an exploitable vulnerability remaining undetected.
- For any inability to comply with security functional requirements that constitutes a potential vulnerability and results in a security incident.
- The associated attack is usually relatively difficult to exploit due to mitigations and/or dependence on specific versions or configurations; and does not provide elevated privileges or significant information benefits.

Low (Minor)

- For any inability to comply with the assurance requirements but which has a temporary fix, workaround or countermeasure; and may result in a Security Warning/Notice.
- Any associated attack requires local or physical access; and it has very little security impact.