

[NEWS] Sybase ASE Remote Password Array Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0094.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/23/03

To: list@securiteam.com

Date: 23 Nov 2003 14:20:27 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Sybase ASE Remote Password Array Denial of Service

SUMMARY

<<http://www.sybase.com>> Sybase Adaptive Server Enterprise (ASE) 12.5 is susceptible to a denial of service attack when a login is made with an invalid remote password array. A valid login is required to exploit this vulnerability.

DETAILS

Vulnerable systems:

- * Sybase ASE version 12.5

Immune systems:

- * Sybase version 11.0.3.3
- * Sybase ASE version 12.5 ESD#2 (Electronic Software Distribution)

Technical details:

Connecting to Sybase Adaptive Server Enterprise (ASE) 12.5 with a valid login (correct user ID and password) and an invalid remote password array causes an access violation on the server, resulting in a denial of service in the child thread or process. On Windows, which spawns threads for each

Securiteam: [NEWS] Sybase ASE Remote Password Array Denial of Service

client, the server will stop responding to all commands, including new login requests. On systems such as Linux, which spawns new child processes for each client, other clients do not appear to be affected. However, an attacker could cause an effective DoS on new clients by rapidly exploiting new child processes as they are launched, denying other clients the ability to log in.

The remote password array is included in the TDS LOGINREC structure and is of the format:

```
byte first server name length
byte[ ] first server name
byte first password length
byte[ ] first password
byte next server name length
...
byte total length of remote password array
```

By specifying invalid lengths, a heap overflow can be triggered. We believe the possibility of arbitrary remote code execution is unlikely in this case, but the possibility has not been ruled out.

ADDITIONAL INFORMATION

The original advisory is available from:

<<http://www.rapid7.com/advisories/R7-0016.html>>
<http://www.rapid7.com/advisories/R7-0016.html>.

The information has been provided by <<mailto:advisory@rapid7.com>> Rapid 7 Security Advisories.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.