

[NEWS] Computer Associates BrightStor HSM Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-10/msg00000.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 1 Oct 2007 08:41:25 +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>

Computer Associates BrightStor HSM Multiple Vulnerabilities

SUMMARY

Computer Associates <<http://www3.ca.com/solutions/Product.aspx?ID=5586>> BrightStor Hierarchical Storage Manager (HSM) is an application used to create a tiered storage solution for enterprises that require on demand access to large quantities of data. The HSM caches frequently used files on hard drives for fast access, and stores seldom used files on tape. Access to files stored on tape is transparent to the client applications. The CsAgent process (CsAgent.exe) is a component of the HSM suite, and listens on TCP port 2000.

Remote exploitation of multiple buffer overflow vulnerabilities in Computer Associates International Inc.'s (CA) BrightStor HSM allows attackers to execute arbitrary code with SYSTEM privileges.

DETAILS

Vulnerable Systems:

- * Computer Associates BrightStor HSM version r11.5.

These problems specifically exist within various command handlers in the

[NEWS] Computer Associates BrightStor HSM Multiple Vulnerabilities

CsAgent service. There are eleven command handlers that contain one or more stack based buffer overflow vulnerabilities each. All of these vulnerabilities are simple sprintf() calls that overflow fixed size stack buffers with attacker supplied data.

Additionally, there are five command handlers that are vulnerable to integer overflow vulnerabilities. In addition to this, the function responsible for reading in and dispatching a request to the appropriate handler also contains an integer overflow vulnerability. In each case, a 32-bit integer is taken from the packet and either added or multiplied to determine how much memory to allocate. When these calculations cause an integer wrap, a heap buffer of insufficient size is allocated. Later, a heap overflow occurs when filling the buffer.

Exploitation of these vulnerabilities results in the execution of arbitrary code with SYSTEM privileges. Unsuccessful attempts will crash the service, but it will be restarted by a watchdog process soon thereafter.

In order to exploit this vulnerability, an attacker must be able to establish a TCP session on port 2000 with the vulnerable host. No authentication is required.

Vendor Status:

Computer Associates has addressed these vulnerabilities with the release of version r11.6. For more information, consult CA's security notice at the following URL.

<<http://supportconnectw.ca.com/public/bstorhsm/infodocs/bstorhsm-secnot.asp>>
<http://supportconnectw.ca.com/public/bstorhsm/infodocs/bstorhsm-secnot.asp>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5082>>
CVE-2007-5082
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5083>>
CVE-2007-5083

Disclosure Timeline:

- * 04/13/2007 Initial vendor notification
- * 04/13/2007 Initial vendor response
- * 09/27/2007 Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.
The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=601>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=601>

=====

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

=====

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.