

# [NEWS] Computer Associates iTechnology iGateway Service Content-Length Buffer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00082.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 25 Jan 2006 09:59:28 +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 iTechnology iGateway Service Content-Length Buffer  
Overflow

---

## SUMMARY

" <<http://www.ca.com/>> iTechnology is an integration technology which provides standard web service interfaces to third-party products, exposing normalized security event data and information in XML format."

By using negative buffer length with Computer Associates iTechnology iGateway Service attackers can execute arbitrary code.

## DETAILS

### Vulnerable Systems:

- \* iTechnology iGateway version 4.0.051215 and prior
- \* Advantage Data Transformer (ADT) R2.2
- \* BrightStor ARCserve Backup r11.5
- \* BrightStor ARCserve Backup r11.1
- \* BrightStor ARCserve Backup for Windows r11
- \* BrightStor Enterprise Backup 10.5
- \* BrightStor ARCserve Backup v9.01
- \* BrightStor ARCserve Backup Laptop & Desktop r11.1

## [NEWS] Computer Associates iTechnology iGateway Service Content–Length Buffer Overflow

- \* BrightStor ARCserve Backup Laptop & Desktop r11
- \* BrightStor Process Automation Manager r11.1
- \* BrightStor SAN Manager r11.1
- \* BrightStor SAN Manager r11.5
- \* BrightStor Storage Resource Manager r11.5
- \* BrightStor Storage Resource Manager r11.1
- \* BrightStor Storage Resource Manager 6.4
- \* BrightStor Storage Resource Manager 6.3
- \* BrightStor Portal 11.1
- \* eTrust Audit 1.5 SP2 (iRecorders and ARIES)
- \* eTrust Audit 1.5 SP3 (iRecorders and ARIES)
- \* eTrust Audit 8.0 (iRecorders and ARIES)
- \* eTrust Admin 8.1
- \* eTrust Identity Minder 8.0
- \* eTrust Secure Content Manager (SCM) R8
- \* eTrust Integrated Threat Management (ITM) R8
- \* eTrust Directory, R8.1 (Web Components Only)
- \* Unicenter CA Web Services Distributed Management R11
- \* Unicenter AutoSys JM R11
- \* Unicenter Management for WebLogic / Management for WebSphere R11
- \* Unicenter Service Delivery R11
- \* Unicenter Service Level Management (USLM) R11
- \* Unicenter Application Performance Monitor R11
- \* Unicenter Service Desk R11
- \* Unicenter Service Desk Knowledge Tools R11
- \* Unicenter Service Fulfillment 2.2
- \* Unicenter Service Fulfillment R11
- \* Unicenter Asset Portfolio Management R11
- \* Unicenter Service Matrix Analysis R11
- \* Unicenter Service Catalog/Fulfillment/Accounting R11
- \* Unicenter MQ Management R11
- \* Unicenter Application Server Management R11
- \* Unicenter Web Server Management R11
- \* Unicenter Exchange Management R11

### Immune Systems:

- \* iTechnology iGateway version 4.0.051230

The vulnerability specifically exists in the iGateway service that listens on port 5250 for standard HTTP or SSL traffic. The iGateway service fails to properly handle negative HTTP Content–Length values. iGateway parses the negative content–length value from an HTTP request and uses the value directly in a malloc() heap allocation call. By supplying negative values, the heap allocation call will return a very small buffer. Subsequent to the malloc() call, a memcpy of the supplied URI into the allocated buffer can overflow into the heap. A remote attacker can send a request with a very large URI and a negative content–length to corrupt the heap and potentially execute arbitrary code.

Successful exploitation of this vulnerability allow remote attackers to execute arbitrary code with SYSTEM level permissions. The iTechnology

[NEWS] Computer Associates iTechnology iGateway Service Content–Length Buffer Overflow

package is distributed with various Computer Associates eTrust brand software. Any attacker who can reach port 5250 on an affected host can attempt to exploit this vulnerability.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3653>>  
CVE-2005-3653

Disclosure Timeline:

11/15/2005 – Initial vendor notification  
11/15/2005 – Initial vendor response  
01/23/2006 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@xxxxxxxxxxxxxxxxxxxx>> iDEFENSE Labs.

The original article can be found at:

<<http://www.idefense.com/intelligence/vulnerabilities/display.php?id=376>>

<http://www.idefense.com/intelligence/vulnerabilities/display.php?id=376>

The vendor advisory can be found at:

<[http://supportconnectw.ca.com/public/ca\\_common\\_docs/igatewaysecurity\\_notice.asp](http://supportconnectw.ca.com/public/ca_common_docs/igatewaysecurity_notice.asp)>

[http://supportconnectw.ca.com/public/ca\\_common\\_docs/igatewaysecurity\\_notice.asp](http://supportconnectw.ca.com/public/ca_common_docs/igatewaysecurity_notice.asp)

=====

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@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====  
=====

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.

- 
- Prev by Date: [\*\[NT\] CounterPath eyeBeam SIP Buffer Overflow\*](#)
  - Next by Date: [\*\[UNIX\] Fetchmail Bouncing Message DoS\*](#)
  - Previous by thread: [\*\[NT\] CounterPath eyeBeam SIP Buffer Overflow\*](#)
  - Next by thread: [\*\[UNIX\] Fetchmail Bouncing Message DoS\*](#)
  - Index(es):

- ◆ *Date*
- ◆ *Thread*