

# [NT] CA CleverPath SQL Injection

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00032.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 25 Apr 2007 16:58:03 +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>

-----

## CA CleverPath SQL Injection

---

### SUMMARY

The CA Clever Path Portal is a customizable portal for aggregation and integration of data and applications. It is integrated into multiple CA products including various Unicenter components. The CA CleverPath utilizes a back end Database for storing data and allows usage of either built in or external Database.

After identifying in CleverPath an irregular behavior when modifying query parameters in the search mechanism, Hacktics has conducted a research of identifying an SQL Injection vulnerability in the implementation of the search query construction.

### DETAILS

By modifying certain parameters in the execute search URL, it was possible to cause the application to send to the database queries that are different than those originally intended by the search engine, and as a result retrieving the entire database contents according to the application user permissions scheme in the database.

Note: Due to the diversity of possible Database implementations for

## [NT] CA CleverPath SQL Injection

CleverPath, the actual level of possible exploitation may vary between different systems.

### Exploit Details:

Due to the complexity of the required syntax, the identified SQL injection does not allow for trivial exploitation such as UNION SELECT. However, data can be still retrieved using Binary Search techniques.

For detailed technical description and exploit please visit  
<<http://www.hacktics.com/AdvCleverPathApr07.html>>  
<http://www.hacktics.com/AdvCleverPathApr07.html>

### Solution:

CA Has been notified of this vulnerability on January 18th, and is releasing a patch together with the publication of the vulnerability.

## ADDITIONAL INFORMATION

The information has been provided by <<mailto:irene@xxxxxxxxxxxxx>> Irene Abezgauz.

The original article can be found at:

<<http://www.hacktics.com/AdvCleverPathApr07.html>>  
<http://www.hacktics.com/AdvCleverPathApr07.html>

=====

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

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

=====

=====

### 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.