

# CA eTrust Antivirus 7.0 – System account lockout

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-07/0002.html>

---

**From:** Geoff Vass (*geoff\_at\_CADZOW.COM.AU*)

**Date:** 06/28/03

Date: Sat, 28 Jun 2003 17:33:09 +0930  
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Greets. Just a heads-up for anybody interested.

Computer Associates' eTrust Antivirus 7.0 (aka InoculateIT) has a feature which locks out a user account for a specified time if the user writes infected files to the server ("quarantine"). An administrator may remove the quarantine manually or the quarantine expires automatically when the time is up. The online help states that the Administrator account will not be locked out.

eTrust Antivirus also has an email add-on option for Exchange which uses the local VSAPI in Exchange to scan attachments.

How these two come together is this: Exchange Server appears to submit messages to VSAPI by writing them to the file system first. eTrust scans the file. Exchange forwards the new file (cleaned or replaced) to the user. However in the meantime the Realtime scanner detects the original infected file and this triggers the account lockout on System.

The log files show:

```
"The Win32.Bugbear.B:corrupt was detected in  
C:\...NTFS_C362EB1001C332EE00000598.EML<9.... Machine: SERVER, User: NT  
AUTHORITY\SYSTEM. File Status: Infected  
User (NT AUTHORITY\SYSTEM) quarantined for 90 minutes."
```

Thereafter processes requiring System access will be denied, including authentication. Users cannot log on to the server either remotely or locally (until the Quarantine expires). Existing authenticated users can still access network resources provided they don't do anything that requires authentication.

eTrust Antivirus 7.0.139 (Admin Server)  
eTrust Antivirus 7.0.343 (Exchange Option)  
Windows 2000 Server SP3  
Exchange 2000 SP3 (6249.4)

There are probably lots of other scenarios and products where this can

