[UNIX] Courier−IMAP Remote Format String Vulnerability

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2004−08/0068.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 08/18/04

```
To: list@securiteam.com
Date: 18 Aug 2004 19:40:45 +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/mailinglist.html

− − − − − − − − −

Courier−IMAP Remote Format String Vulnerability
−−−

```
    int len;

    // print into buffer to be able to replace control and other
    // unwanted chars.
    vsnprintf( buf, DEBUG_MESSAGE_SIZE, fmt, ap );
    len = strlen( buf );

    // replace nonprintable chars by dot
    for( i=0 ; i<len ; i++ )
          if( !isprint(buf[i]) )
                buf[i] = '.';

    // emit it
    fprintf( stderr, buf ); // <− Format String Vulnerability
    fprintf( stderr, "\n" );
}
```

The 'buf' variable utilized in the fprintf() call is attacker−controlled and can contain format string modifiers allowing an attacker to manipulate the stack and eventually execute arbitrary code.

Analysis:
Successful exploitation does not require authentication thereby allowing any remote attacker to execute arbitrary code under the privileges of the user that the IMAP daemon runs as. The vulnerable function auth_debug() is only called if login debugging is enabled requiring that the 'DEBUG_LOGIN' be set to either '1' or '2' in the imapd configuration file.

Workaround:
Disable the login debugging option of Courier−IMAP. This can be accomplished by setting 'DEBUG_LOGIN' to '0' in the configuration file usually located at /usr/lib/courier−imap/etc/imapd.

Vendor response:
This issue has been resolved in the latest version of Courier IMAP (v3.0.7). As well, the default setting of 'DEBUG_LOGIN' is '0'.

CVE Information:
<http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2004−0777>
CAN−2004−0777

Disclosure timeline:
08/10/2004 Initial vendor contact
08/10/2004 iDEFENSE clients notified
08/11/2004 Initial vendor response
08/18/2004 Public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<mailto:idlabs−advisories@idefense.com> iDEFENSE.

The original article can be found at:
<http://www.idefense.com/application/poi/display?id=131&type=vulnerabilities&flashstatus=true>
http://www.idefense.com/application/poi/display?id=131&type=vulnerabilities&flashstatus=true

==========

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.