

# [Full-disclosure] iDEFENSE Security Advisory 12.06.05: Ipswitch IMail IMAP List Command DoS Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-12/msg00308.html>

---

- *From:* "labs-no-reply@xxxxxxxxxxxx" <labs-no-reply@xxxxxxxxxxxx>
  - *Date:* Tue, 06 Dec 2005 18:06:39 -0500
- 

Ipswitch IMail IMAP List Command DoS Vulnerability

iDEFENSE Security Advisory 12.06.05  
[www.idefense.com/application/poi/display?id=347&type=vulnerabilities](http://www.idefense.com/application/poi/display?id=347&type=vulnerabilities)  
December 6, 2005

## I. BACKGROUND

Ipswitch Imail Server is an email server that is part of the IpSwitch Collaboration suit. Imail Supports POP3, SMTP, IMAP and web based email access. More Information can be located on the vendor s site at:

<http://www.ipswitch.com/Products/collaboration/index.html>

## II. DESCRIPTION

Remote exploitation of a denial of service (DoS) vulnerability in Ipswitch Inc.'s Imail IMAP server allows attackers to crash the target service, thereby preventing legitimate use.

The problem specifically exists in handling long arguments to the LIST command. When a LIST command of approximately 8000 bytes is supplied, internal string parsing routines can be manipulated in such a way as to reference non-allocated sections of memory. This parsing error results in an unhandled access violation, forcing the daemon to exit.

### III. ANALYSIS

Exploitation allows remote attackers to crash vulnerable IMAP servers and thereby prevent legitimate usage. The LIST command is only available post authentication and therefore valid credentials are required to exploit this vulnerability.

### IV. DETECTION

iDEFENSE has confirmed the existence of this vulnerability in Ipswitch IMail 8.2.

### V. WORKAROUND

As this vulnerability is exploited after authentication occurs, ensuring that only trusted users have accounts can mitigate the risk somewhat. As a more effective workaround, consider limiting access to the IMAP server by filtering TCP port 143. If possible, consider disabling IMAP and forcing users to use POP3.

### VI. VENDOR RESPONSE

Ipswitch Collaboration Suite 2.02 has been released to address this issue and is available for download at: