[NT] Ipswitch IMail IMAP Vulnerabilities (Multiple Buffer Overflow, Multiple DoS, Directory Traversal)

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2005−05/0131.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 05/25/05

```
To: list@securiteam.com
Date: 25 May 2005 11:39:48 +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

− − − − − − − − −

Ipswitch IMail IMAP Vulnerabilities (Multiple Buffer Overflow, Multiple DoS, Directory Traversal)
−−−

Immune Systems:
* Ipswitch IMail Server 8.2 Hotfix 2

SELECT Command DoS:
Remote exploitation of a denial of service vulnerability in Ipswitch Inc.'s IMail IMAP server allows attackers to crash the target service thereby preventing legitimate usage.

The problem specifically exists in the handling of long arguments to the SELECT command. When a string approximately 260 bytes in size is supplied a stack−based buffer overflow occurs that results in an unhandled access violation forcing the daemon to exit. The issue is not believed to be further exploitable.

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

LSUB DoS:
Remote exploitation of a denial of service (DoS) vulnerability in Ipswitch Inc.'s IMail IMAP daemon allows attackers to cause 100 percent CPU use on the server, thereby preventing legitimate users from retrieving e−mail.

The problem specifically exists within IMAPD32.EXE upon parsing a malformed LSUB command. An attacker can cause the daemon to produce heavy load by transmitting a long string of NULL characters to the 'LSUB' IMAP directive. This, in turn, causes an infinite loop, eventually exhausting all available system resources and causing a denial of service.

Exploitation allows unauthenticated remote attackers to render the IMAP server useless, thereby preventing legitimate users from retrieving e−mail. This attack takes few resources to launch and can be repeated to ensure that an unpatched system is unable to recover. Exploitation requires a valid IMAP account, thus limiting the impact of this vulnerability.

Directory Traversal:
Remote exploitation of a directory traversal vulnerability in Ipswitch Inc.'s IMail Web Calendaring server allows attackers to read arbitrary files with System privileges.

The problem specifically exists because of a flaw in the handling of requests for nonexistent JavaScript (jsp) files. By requesting a nonexistent jsp file followed by a question mark, several sequences of "..\" and then the path to a file on the system, an attacker can read arbitrary files remotely without any authentication.

Proof of Concept:
The following query demonstrates how the system's boot.ini file may be retrieved:

```
GET /bla.jsp?\..\..\..\..\..\..\..\..\..\..\..\..\boot.ini HTTP/1.0
Connection: Close
Host: example.com
User−Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Pragma: no−cache
```

Successful exploitation allows remote attackers to retrieve arbitrary files from the target host. Exploitation does not require authentication and does not require exploit code, as a user can simply type the malicious query in a web browser.

LOGIN Remote Buffer Overflow:
Remote exploitation of several buffer overflow vulnerabilities in Ipswitch Inc.'s IMail IMAP server allows attackers to execute arbitrary code with System privileges.

The first vulnerability specifically exists in the handling of a long username to the LOGIN command. A long username argument of approximately 2,000 bytes will cause a stack based Unicode string buffer overflow providing the attacker with partial control over EIP. As this vulnerability is in the LOGIN command itself, valid credentials are not required.

The second vulnerability also exists in the handling of the LOGIN command username argument, however it lends itself to easier exploitation. If a large username starting with one of several special characters is specified, a stack overflow occurs, allowing an attacker to overwrite the saved instruction pointer and control execution flow.

Included in the list of special characters are the following: % : * @ &,
Both of these vulnerabilities can lead to the execution of arbitrary code.

Successful exploitation allows remote attackers to execute arbitrary code with System privileges. Valid credentials are not required to for exploitation, which heightens the impact of this vulnerability.

STATUS Remote Buffer Overflow:
Remote exploitation of a buffer overflow vulnerability in Ipswitch Inc.'s IMail IMAP server allows attackers to execute arbitrary code with System privileges.

The vulnerability specifically exists in the handling of a long mailbox name to the STATUS command. A long mailbox name argument will cause a stack based buffer overflow, providing the attacker with full control over the saved return address on the stack. Once this has been achieved, execution of arbitrary code becomes trivial. As this vulnerability is in the STATUS command, which requires that a session is authenticated, valid credentials are required.

Successful exploitation allows remote attackers to execute arbitrary code with System privileges. Valid credentials are required for exploitation,

which lessens the impact of this vulnerability.

Workaround:
* Consider limiting access to the IMAP server by filtering TCP port 143. If possible, consider disabling IMAP and forcing users to use POP3.
* Limit access to the Web Calendaring server by allowing only trusted hosts to access TCP port 8484, the default port for Web Calendaring. If the Web Calendaring service is not required, disable it entirely.

Vendor Status:
The vendor has released the following patch to fix this vulnerability:
<ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/imail82hf2.exe>
ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/imail82hf2.exe

CVE Information:
<http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1249>
CAN−2005−1249
<http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1252>
CAN−2005−1252
<http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1254>
CAN−2005−1254
<http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1255>
CAN−2005−1255
<http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1256>
CAN−2005−1256

Disclosure Timeline:
04/15/2005 − Initial vendor notification
05/10/2005 − Initial vendor response
05/24/2005 − Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<mailto:idlabs−advisories@idefense.com> idlabs.
The original article can be found at:
<http://www.idefense.com/application/poi/display?id=241&type=vulnerabilities>
http://www.idefense.com/application/poi/display?id=241&type=vulnerabilities,

<http://www.idefense.com/application/poi/display?id=242&type=vulnerabilities>
http://www.idefense.com/application/poi/display?id=242&type=vulnerabilities,

<http://www.idefense.com/application/poi/display?id=243&type=vulnerabilities>
http://www.idefense.com/application/poi/display?id=243&type=vulnerabilities,

<http://www.idefense.com/application/poi/display?id=244&type=vulnerabilities>
http://www.idefense.com/application/poi/display?id=244&type=vulnerabilities,

<http://www.idefense.com/application/poi/display?id=245&type=vulnerabilities>
http://www.idefense.com/application/poi/display?id=245&type=vulnerabilities
The Vendor advisory can be found at:

<http://www.ipswitch.com/support/imail/releases/imail_professional/im82hf2.html>
http://www.ipswitch.com/support/imail/releases/imail_professional/im82hf2.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@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.