

[NT] Ipswitch Multiple Vulnerabilities (IMail IMAP LIST Command DoS, Collaboration Suite SMTP Format String)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00029.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 11 Dec 2005 11:55:45 +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/maillinglist.html>

Ipswitch Multiple Vulnerabilities (IMail IMAP LIST Command DoS,
Collaboration Suite SMTP Format String)

SUMMARY

" <<http://www.ipswitch.com/products/collaboration/index.asp>> Ipswitch Collaboration Suite provides e-mail and real-time collaboration, calendar and contact list sharing, and protection from spam and viruses, all delivered in an easy to use suite."

Remote exploitation of a denial of service (DoS) vulnerability in Ipswitch Imail IMAP server allow attackers to crash the target service. Remote exploitation of a format string vulnerability in Ipswitch IMail allows remote attackers to execute arbitrary code.

DETAILS

Vulnerable Systems:

- * Ipswitch IMail version 8.2
- * Ipswitch Collaboration Suite 8.20

[NT] Ipswitch Multiple Vulnerabilities (IMail IMAP LIST Command DoS, Collaboration Suite SMTP Format String)

Immune Systems:

* Ipswitch Collaboration Suite 2.02

IMail IMAP List Command DoS:

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.

Exploitation allow 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.

Workaround:

As this vulnerability is exploited after authentication occurs, ensuring that only trusted users have accounts can mitigate the risk somewhat. If possible, consider disabling IMAP and forcing users to use POP3.

Collaboration Suite SMTP Format String:

The vulnerability specifically exists due to improper use of functions which allow format specifiers in the SMTP service included with ICS. Remote attackers can supply format string values to certain string functions to cause memory corruption leading to remote code execution. The vulnerability may be exploited by supplying specially crafted strings to any of the following SMTP commands: EXPN, MAIL, MAIL FROM, RCPT TO. All of the commands are handled by the same function which parses user-supplied input strings. The following debugger session shows a backtrace with user-supplied strings as values. With properly constructed input value, the strings would be interpreted as memory addresses that would be executed upon returning from the current function.

```
[..]
00A7F370 006020A0
00A7F374 00A7F634 ASCII 5B,"192.168.242.1] MAIL
FROM:C:\apps\Ipswitch\Collaboration
Suite\IMail\spool\T94e8013e00000005"
00A7F378 00000000
00A7F37C 00000000
00A7F380 7C34FC0B RETURN to MSVCR71.7C34FC0B from MSVCR71.write_char
00A7F384 00602048
00A7F388 00A7F648 ASCII 20,"FROM:C:\apps\Ipswitch\Collaborat"
[..]
```

Successful exploitation of the format string vulnerability allows unauthenticated remote attackers to execute arbitrary code. Ipswitch mail services are commonly configured to allow untrusted access. The use of a firewall or other mitigating strategy is highly recommended due to the nature of this vulnerability. The IMail SMTP server is installed by default.

[NT] Ipswitch Multiple Vulnerabilities (IMail IMAP LIST Command DoS, Collaboration Suite SMTP Format String)

[NT] Ipswitch Multiple Vulnerabilities (IMail IMAP LIST Command DoS, Collaboration Suite SMTP Format String)

Vendor Status:

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

<<http://www.ipswitch.com/support/ics/updates/ics202.asp>>
<http://www.ipswitch.com/support/ics/updates/ics202.asp>

IMail Server 8.22 Patch has been released to address this issue and is available for download at:

<http://www.ipswitch.com/support/imail/releases/imail_professional/im822.asp>
http://www.ipswitch.com/support/imail/releases/imail_professional/im822.asp

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2923>>
CAN-2005-2923
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2931>>
CAN-2005-2931

Disclosure Timeline:

09/08/2005 Initial vendor notification
09/13/2005 Initial vendor response
10/06/2005 Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@xxxxxxxxxxxxxxxxxxxx>> iDEFENSE.

The original article can be found at:

<<http://www.odefense.com/application/poi/display?id=346&type=vulnerabilities>>
<http://www.odefense.com/application/poi/display?id=346&type=vulnerabilities>,

<<http://www.odefense.com/application/poi/display?id=347&type=vulnerabilities>>
<http://www.odefense.com/application/poi/display?id=347&type=vulnerabilities>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.

- Prev by Date: [*\[NT\] Microsoft Windows Wireless Zero Multiple Vulnerabilities \(Information Disclosure, Authentication Bypass\)*](#)
- Next by Date: [*\[UNIX\] Ethereal OSPF Protocol Dissector Buffer Overflow*](#)
- Previous by thread: [*\[NT\] Microsoft Windows Wireless Zero Multiple Vulnerabilities \(Information Disclosure, Authentication Bypass\)*](#)
- Next by thread: [*\[UNIX\] Ethereal OSPF Protocol Dissector Buffer Overflow*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)