

[UNIX] Ipswitch Collaboration Suite SMTP Server Stack Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00005.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 10 Sep 2006 14:25:50 +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 Collaboration Suite SMTP Server Stack Overflow

SUMMARY

"Ipswitch Collaboration Suite delivers the communication and collaboration tools that small and mid-sized businesses need in an easy to use suite, without the overhead of enterprise systems".

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Ipswitch Collaboration Suite and IMail.

DETAILS

Vulnerable Systems:

- * ICS/IMail Server 2006

Description:

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Ipswitch Collaboration Suite and IMail.

Authentication is not required to exploit this vulnerability.

The specific flaw exists within the SMTP daemon. A lack of bounds checking during the parsing of long strings contained within the

[UNIX] Ipswitch Collaboration Suite SMTP Server Stack Overflow

characters '@' and ':' leads to a stack overflow vulnerability.
Exploitation can result in code execution or a denial of service.

CVE Information:

<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4379>>
CVE-2006-4379

Vendor Status:

Ipswitch has issued an update, version 2006.1, to correct this vulnerability. More details can be found at:

<http://www.ipswitch.com/support/imap/releases/im20061.asp>

Disclosure Timeline:

2006.06.22 – Vulnerability reported to vendor
2006.08.31 – Digital Vaccine released to TippingPoint customers
2006.09.07 – Coordinated public release of advisory

ADDITIONAL INFORMATION

The information has been provided by: the Zero Day Initiative (ZDI). This vulnerability was discovered by an anonymous researcher.

For the original advisory please visit:

<<http://www.zerodayinitiative.com/advisories/ZDI-06-028.html>>
<http://www.zerodayinitiative.com/advisories/ZDI-06-028.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@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.