

[NT] SpeedProject Products ZIP and UUE File Extraction Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0092.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/29/05

To: list@securiteam.com

Date: 29 Nov 2005 11:44:01 +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>

SpeedProject Products ZIP and UUE File Extraction Buffer Overflow

SUMMARY

" <<http://www.speedproject.de/enu/speedcommander/index.html>>

SpeedCommander is a comfortable file manager."

" <<http://www.speedproject.de/enu/squeez/index.html>> Squeez is an

extremely fast file compression application, supporting 13 different compression algorithms."

" <<http://www.speedproject.de/enu/zipstar/index.html>> ZipStar is our FREE archiving application for home users."

Lack of length validation allow attackers to cause the SpeedProject program to execute arbitrary code.

DETAILS

Vulnerable Systems:

* ZipStar version 5.0 Build 4285

* Squeez version 5.0 Build 4285

* SpeedCommander version 11.0 Build 4430

* SpeedCommander version 10.51 Build 4430

Securiteam: [NT] SpeedProject Products ZIP and UUE File Extraction Buffer Overflow

Immune Systems:

- * SpeedCommander version 10.52 Build 4450
- * SpeedCommander version 11.01 Build 4450
- * Squeez version 5.10 Build 4460
- * ZipStar version 5.10 Build 4460

A boundary error exists in CxZIP60.dll and CxZIP60u.dll due to the unsafe use of the "Istrcat()" function when constructing the full pathname of a file that is extracted from a ZIP archive. This can be exploited to cause a stack-based buffer overflow and allows arbitrary code execution when a specially crafted archive is extracted. The vulnerability also exists with CxUux60.dll and CxUux60u.dll library that handles UUE decoding.

Disclosure Timeline:

- 03/11/2005 – Initial vendor notification.
- 03/11/2005 – Initial vendor reply.
- 17/11/2005 – Vendor released fixed versions.
- 24/11/2005 – Public disclosure.

ADDITIONAL INFORMATION

The information has been provided by <mailto:vuln@secunia.com> Secunia Research.

The original article can be found at:
 <<http://secunia.com/advisories/17420/>>
<http://secunia.com/advisories/17420/>

=====

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.