Compression Plus and Tumbleweed EMF
Stack Overflow Security Advisory

Summary

The Compression Plus library is designed to handle de/compression of popular archiving formats such as ARC, ARK, PAK, ARJ, CAB, GZ, LBR, TAR, TAZ, TGZ, Z, ZIP, and ZOO. The code fails to properly validate input while processing specially crafted ZOO files, which results in a stack-based buffer overflow. Software products that implement the Compression Plus library are vulnerable to local or remote code execution, depending on the nature of the calling process.

Affected Software

Due to the modular nature and availability of the Compression Plus code, any programs which load the library and call its ZOO-processing exports are affected by this vulnerability. Exploits have been tested successfully on the following products; however the list is not exhaustive.

Software Title	Version(s)	Vendor & Product URL	Perspective
Compression Plus	All versions	BeCubed Software	N/A
Tumbleweed EMF	All versions	Tumbleweed Communications	Remote
PowerDesk Pro	All versions	VCOM/Ontrack	Local
Drag and Zip, Power File, and Power File Gold	All versions	Canyon Software	Local

Impact

Arbitrary code can be executed on vulnerable systems with a privilege level equal to the calling process, which by default is SYSTEM on Tumbleweed EMF servers. For all others, an attacker's code will run with the privileges of the current logged-in user.

Credit and Contact

Michael Ligh michael.ligh@mnin.org
Greg Sinclair gssincla@nnlsoftware.com
Amanda Wright advisories@ladybugz.net

Exploit Design

There are several factors of this vulnerability that not only increase the simplicity of exploiting affected software, but make it more difficult for a defender to detect or trace the attack. As a result, exploitation can be conducted with high reliability and with little chance of IDS or IPS intervention.

An attacker can supply up to 32KB of custom shell code or any combination of shell code plus binary data (e.g. an additional trojan program) to be executed on the target. There are no limitations involving NULL bytes in the payload. Furthermore, control over EIP can be gained without hard coding addresses on the stack or using NOP instruction sleds.

The specially crafted ZOO files retain compliance with legitimate ZOO file format, so IDS signatures based on protocol anomalies or specific header values will not be sufficient for detection. Email attachment and HTTP/FTP download filtering based on file extension is also not applicable, because the vulnerability is not extension-specific.

The traceability of an attacker's actions can be influenced by routing malicious ZOO files through a series of open SMTP proxies. With the exception of Tumbleweed EMF, which does not require any user interaction to successfully exploit, an attacker would need to convince recipients to open/decompress the ZOO file from within a vulnerable program.

Details

This vulnerability exists because the nNumberOfBytesToRead parameter to ReadFile() is obtained from user-supplied data and there is no check to see if its length exceeds the size of the destination buffer. A value as high as 7FFFh can be passed to ReadFile(), however one must only specify 39Ch bytes to overwrite the function's return pointer on the stack. The following code from a Compression Plus library is shown below to illustrate the vulnerability.

```
.text:1040A71B    movsx   eax, word ptr [ebp+ZooHeader+24h]
.text:1040A71F    push    eax  ; nNumberOfBytesToRead
.text:1040A720    lea     eax, [ebp+var_394]
.text:1040A726    push    eax  ; lpBuffer
.text:1040A727    push    [ebp+ZooHeader+88h]
.text:1040A72A    call    _ReadFileWrapper
```

Remediation

The code should verify that the user-supplied dword at ZooHeader+24h is not larger than the number of bytes reserved for the destination buffer. BeCubed Software has released an updated Compression Plus DLL that complies with this remediation technique. The fix can be obtained from http://www.becubed.com/support.htm. In addition, the Tumbleweed Hotfix can be obtained from https://kb1.tumbelweed.com/article.asp?article=4175&p=2.

Event Timeline

Jul 12, 2006	Began research and testing
Jul 25, 2006	Advisory drafted
Jul 26, 2006	Primary vendor (BeCubed) contacted
Aug 01, 2006	Primary vendor released a fixed DLL
Aug 01, 2006	Secondary vendor(s) contacted
Aug 22, 2006	Tumbleweed releases Hotfix for EMF 6.2.2

Attributions

The scared Scooby Doo image was taken from:
http://www.jecolorie.com.

The code snippet was extracted from the disassembly pane of IDA Pro:
http://www.datarescue.com

License