

RE: Download Accelerator Plus can be tricked to download malicious file

RE: Download Accelerator Plus can be tricked to download malicious file

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-01/msg00070.html>

- *From:* "NaPa" <napa@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 4 Jan 2006 12:58:40 -0600
-

I didn't see this as a DAP fail, is normal to have out because of network configuration, but, how you can make your own Server to be detected as a mirror of the file. I mean if you could do this is that a fact nut by know for me is not a flaw.

What do you think?

-----Mensaje original-----

De: visitbipin@xxxxxxxxxxx [<mailto:visitbipin@xxxxxxxxxxx>]

Enviado el: miércoles, 04 de enero de 2006 11:31

Para: bugtraq@xxxxxxxxxxxxxxxxxxxxx

Asunto: Download Accelerator Plus can be tricked to download malicious file

Product(ONLY TESTED ON): Download Accelerator Plus 7.4.0.2 (unregistered)

Test Environment: Winxp Pro sp2 (patch level latest)

Risk Type: Rare exception

Threat Level: High

Vendor website:www.speedbit.com

POC screenshots: <http://img482.imageshack.us/img482/4205/31uk.jpg>

<http://img425.imageshack.us/img425/4380/15an.jpg>

speedbit.com claims to have 110 million users of DAP world wide and is one of the popular and best download manager for windows. One of its biggest strength to download big files in a faster connection at optimum speed is, it can automatically search for best mirrors and download different parts of the file form multiple location.

BUT Download Accelerator Plus(DAP) may switch its download to a un trusted or malicious website while searching for fastest mirrors for a particular file under certain conditions. If the ACTUAL, trusted host providing the file is DOWN or due to network congestions the users may get and execute a malicious file instead.

I've included two screenshots which should be self explanatory. Check out the url?s in each screenshot and see from where the file is being received at the end.

RE: Download Accelerator Plus can be tricked to download malicious file

RE: Download Accelerator Plus can be tricked to download malicious file

In the screenshot I'm trying to download 'Windows 2003 sp1' from download.microsoft.com but DAP automatically chooses to download it only from ftp.planet.nl as my network was having tooooooo low internet bandwidth at that time.

Further more, on some network/OS there might be rules for MAX CONNECTION PER HOST and (say)if in the network someone is already downloading some file from download.microsoft.com the outcome will surely be a VIRTUAL network congestion for download.microsoft.com within that DMZ.

For my test I used another client computer behind the gateway to send continuous ping (17 different instants) to download.microsoft.com As a result, for my network download.microsoft.com was off the radar. So, in my another computer DAP chooses to download Win2003 sp1 from ftp.planet.nl instead. So, even after my network gained its full throttle... no-wonder DAP was still downloading the file from ftp.planet.nl

My test network setup was a 3 computer PC which was left on default configuration with Winxp sp2 (patchlevel: latest)

Changes: This advisory is slightly modified than the one that I emailed to the vendor about a week back and tried contacting it, but with no response till now!

Result: I was receiving the file from an unknown and un-trusted source which could be infected with a malicious program.

BUT fyi: I haven't researched on HOW and WHERE 'DAP' queries to get other possible mirrors for the particular file.

Conclusion: I insist NOT to use download managers that does the same while downloading important files. Or either force your download manager and check whether the file is being downloaded from the original URL or not.

Regards,
-Bipin Gautam

• **References:**

- ◆ **[Download Accelerator Plus can be tricked to download malicious file](#)**
◇ From: visitbipin

- Prev by Date: **[Contact information for Symantec Vulnerability Management](#)**
- Next by Date: **[Uninformed Journal Release Announcement: Volume 3](#)**
- Previous by thread: **[Download Accelerator Plus can be tricked to download malicious file](#)**
- Next by thread: **[Re: Download Accelerator Plus can be tricked to download malicious file](#)**
- Index(es):
 - ◆ **[Date](#)**
 - ◆ **[Thread](#)**

RE: Download Accelerator Plus can be tricked to download malicious file