7z*.exe allows remote code execution with escalation of privilege

By Stefan Kanthak

Archived: 2026-04-05 15:49:27 UTC

Full Disclosure mailing list archives

Executable installers are vulnerable^WEVIL (case 7): 7z*.exe allows remote code execution with escalation of privilege

---

From: "Stefan Kanthak" <stefan.kanthak () nexgo de>
Date: Tue, 8 Dec 2015 18:33:48 +0100

```
Hi @ll,

the executable installers [°] of 7-Zip (see <http://www.7-zip.org/>)
and ALL self-extracting archives created with 7-Zip are vulnerable:

1. They load and execute a rogue/bogus/malicious UXTheme.dll ['] 
   eventually found in the directory they are started from (the
   "application directory").

   For software downloaded with a web browser this is typically the
   "Downloads" directory: see
   <https://insights.sei.cmu.edu/cert/2008/09/carpet-bombing-and-directory-poisoning.html>,
   <http://blog.acrossecurity.com/2012/02/downloads-folder-binary-planting.html>
   and <http://seclists.org/fulldisclosure/2012/Aug/134>

   If UXTheme.dll gets planted in the users "Downloads" directory
   per "drive-by download" this vulnerability becomes a remote code
   execution.

   Due to an application manifest embedded in the executable which
   specifies "requireAdministrator" or the "installer detection" (see
   <https://technet.microsoft.com/en-us/library/dd835540.aspx#BKMK_InstDet>)
   of Windows' "user account control" executable installers are
   typically started with administrative privileges ("protected"
   administrators are prompted for consent, unprivileged standard
   users are prompted for an administrator password); execution of
```

```
   UXTheme.dll then results in an escalation of privilege!


Proof of concept/demonstration:
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

1. visit <http://home.arcor.de/skanthak/sentinel.html>, download
   <http://home.arcor.de/skanthak/download/SENTINEL.DLL> and store
   it as UXTheme.dll in your "Downloads" directory;

   Note: this is the 32-bit DLL; the 64-bit DLL is available in
   <http://home.arcor.de/skanthak/download/SENTINEL.CAB>

2. download <http://www.7-zip.org/a/7z1512.exe> and store it in the
   "Downloads" directory;

3. run 7z1512.exe from the "Downloads" directory;

4. notice the message box displayed from UXTheme.dll placed in step 1.


Mitigation(s):
~~~~~~~~~~~~~~

0. DON'T USE EXECUTABLE INSTALLERS [°]!

   If your favourite applications are not distributed in the native
   installer package format of the resp. target platform: ask^WURGE
   their vendors/developers to provide native installation packages.
   If they don't: dump these applications, stay away from such cruft!

1. Turn off UAC's privilege elevation for standard users and installer
   detection for all users:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
   "ConsentPromptBehaviorUser"=dword:00000000 ; Automatically deny elevation requests
   "EnableInstallerDetection"=dword:00000000

   See <https://technet.microsoft.com/en-us/library/dd835564.aspx#BKMK_RegistryKeys>

2. NEVER execute files in UNSAFE directories (like "Downloads" and
   and "%TEMP%")!

3. Deny execution (at least) in the "Downloads" directories and all
   "%TEMP%" directories and their subdirectories:

   * Add the NTFS ACE "(D;OIIO;WP;;;WD)" meaning "deny execution of
```

```
     files in this directory for everyone, inheritable to all files
     in all subdirectories" (use CACLS.EXE /S:<SDDL> for example);

   * Use "software restriction policies" resp. AppLocker.

   Consider to apply either/both to every "%USERPROFILE%" as well as
   "%ALLUSERSPROFILE%" alias %ProgramData%" and "%PUBLIC%": Windows
   doesn't place executables in these directories and beyond.

   See <http://home.arcor.de/skanthak/safer.html> as well as
   <http://mechbgon.com/srp/> plus
   <http://csrc.nist.gov/itsec/SP800-68r1.pdf>,
   <https://www.nsa.gov/ia/_files/os/win2k/application_whitelisting_using_srp.pdf>
   or <https://books.google.de/books?isbn=1437914926> and finally
   <http://www.asd.gov.au/infosec/top35mitigationstrategies.htm>!


stay tuned
Stefan Kanthak


PS: see <http://seclists.org/fulldisclosure/2015/Nov/101> (resp. the
    not yet finished <http://home.arcor.de/skanthak/!execute.html>)
    for more details!

PPS: the case numbers are not in chronological order.


[°] Self-extracting archives and executable installers are flawed^W
    b(rainde)ad in concept and dangerous in practice.

    DON'T USE SUCH CRUFT!
    ALWAYS use the resp. target platforms native package and archive
    format.

    For Windows these are .INF (plus .CAB) and .MSI (plus .CAB),
    introduced 20 years ago (with Windows 95 and Windows NT4) resp.
    16 years ago (with Office 2000).

    Both .INF and .MSI are "opened" by programs residing in
    %SystemRoot%\System32\ which are therefore immune to this kind
    of "DLL and EXE Search Order Hijacking" attack.
    Since both .INF and .MSI access the contents of .CAB directly
    they eliminate the attack vector "unsafe temporary directory"
    too.

['] A well-known (trivial, easy to exploit and easy to avoid) and
```

```
    well-documented vulnerability: see
    <https://capec.mitre.org/data/definitions/471.html>,
    <https://technet.microsoft.com/en-us/library/2269637.aspx>,
    <https://msdn.microsoft.com/en-us/library/ff919712.aspx> and
    <https://msdn.microsoft.com/en-us/library/ms682586.aspx>


Timeline:
~~~~~~~~~

2015-11-18    vulnerability report sent to author

              NO ANSWER, not even an acknowledgement of receipt

2015-12-05    vulnerability report resent to author

2015-12-05    response from author:
              "What about another exe installers?
               Firefox, Chrome, Skype, WinRAR and others.
               All of them use exe installers."

2015-12-05    other executable installers don't matter here; see
              but <https://bugzilla.mozilla.org/show_bug.cgi?id=792106> and
              <https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/>

2015-12-06    several more lame and COMPLETELY clueless responses
              from author showing that he didn't even read the
              sources referenced here

2015-12-08    report published


_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

Current thread:

- **Executable installers are vulnerable^WEVIL (case 7): 7z*.exe allows remote code execution with escalation of privilege** *Stefan Kanthak (Dec 09)*

Source: http://seclists.org/fulldisclosure/2015/Dec/34