University of Tartu
Institute of Computer Science
Informatics

Essay by Kaur Karus
“CVE-2016-0121 vulnerability”

Supervisor: Meelis Roos

Tartu 2016
Introduction
CVE-2016-0121 is an ‘OpenType font parsing vulnerability’ type security threat. This means that the
issue lies in how OpenType fonts are read and analyzed in different applications. CVE-2016-0121 is
specific to Microsoft Windows operating systems ranging from Vista to 10, including Server editions.
To clearly understand how parsing a font can have security implications, a further explanation of the
OpenType font format is in order.

OpenType font format
Fonts specified by the OpenType font format are not sets of characters, but sets of glyphs. Glyphs
specify how characters or sets of characters can look like, even allowing a single character to be
presented by different glyphs. This allows for optional enhancements to any text, such as affecting
ligatures, kerning, or supporting diverse languages such as Arabic, where how a single character looks
depends on its position in a word. To attain this flexibility, the fonts include scripts which helps text
processing applications adjust how the text looks. The main advantages of using OpenType fonts are
the forenamed flexibility and customization options per font and the fact that any single OpenType
font format file can be used on any operating system. Because of these advantages, OpenType fonts
are commonly used.

Exploit
Any person can create their own OpenType font and put it online for sharing or use it in a document
or website. User-made fonts can include custom scripts that can have adverse effects. A fault in the
Windows Adobe Type Manager Library allows for these scripts to run. A malicious script can, with the
help of running Adobe Type Manager Font Driver (ATMFD) cause malicious code to be run in kernel
privileges. This is caused by the ATMFD creating a font buffer underflow or overflow during font
processing. An attacker can prepare the font buffer in such a way that processing the buffer will cause
controlled content to be written in the system’s random access memory in positions outside the font
buffer. When the newly created code is later processed, it will be run with elevated privileges. Other
similar vulnerabilities can cause RAM data leaks to third parties and deliberate system crashes. CVE-
2016-0121 allows used fonts to execute malicious code with elevated privileges, leading to potential
loss of stored data, sharing of stored data to third parties, install software, etc. Windows 10 limits the
script to run in an AppContainer sandbox with limited privileges. A failed attack using the CVE-2016-
0121 vulnerability causes the system to stop responding or, in the case of Windows 10, the program
reading the malicious font to stop responding (also known as CVE-2016-0120 vulnerability).

Solutions
One proposed workaround is renaming or deleting atmfd.dll in the System32 folder or disabling Adobe
Type Manager Font Driver from the registry. Disabling ATMFD can cause issues displaying OpenType
fonts properly.

Windows 10 includes a Blocking Untrusted Fonts feature, which when turned on will disallow the Font
Driver from parsing OpenType fonts that have not been previously manually installed by the user and
thus marked as ‘safe’. In this case only user-made fonts that have been added to a document or web
page that the potential victim opens will not be displayed properly, thereby removing the risk to the
user’s system. To turn on this feature, the user has to use a registry editor to add a MitigationOptions
(64-bit QWORD Value) key to the HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\Kernel\ path. While this solves the problem as far as executing code from potentially
dangerous sources, it forces the user to manually install new fonts. It does not protect against a user who decides to install a font which can be used to abuse the vulnerability by documents or web pages.

Microsoft has also deployed a patch which attempts to prevent code that abuses this specific vulnerability from being successfully parsed. As such, the vulnerability CVE-2016-0121 is considered fixed. However, since similar vulnerabilities have been found on a yearly basis for almost a decade, custom OpenType fonts continue to be a security threat. As always, it is recommended to not accept or execute files from unknown sources nor follow links provided by unknown sources.

Literature

2. OpenType Layout description: [https://www.microsoft.com/typography/otspec/TTOCHAP1.htm](https://www.microsoft.com/typography/otspec/TTOCHAP1.htm)
3. OpenType Glyph processing description: [https://www.microsoft.com/typography/developers/opentype/over.htm](https://www.microsoft.com/typography/developers/opentype/over.htm)