## Summary

To WinRAR users: most of latest publications about WinRAR vulnerability are heavily hyperbolized. WinRAR itself is not affected and you can use it to unpack all kinds of archives including self-extracting (.exe) as long as you unpack them with WinRAR and do not run them. The newly discovered issue does not add new risks to SFX archives (.exe files). You still need to run them only if they are received from a trustworthy source, as before. No patches for WinRAR are needed. If you have not installed Windows MS14-064 security update, please do it. It is important for entire Windows security, not just for WinRAR SFX.

To journalists and security experts: .exe files can run the executable code. They can even download and run files, really. Exe files are potentially dangerous. Any exe files. But .rar and .zip files are not .exe. Unpatched Windows systems are not safe. Thank you.

## Long story

Since new publications about a supposed WinRAR self-extracting (SFX) archives vulnerability are appearing, we would like to provide more details about this issue.

The entire attack is based on vulnerabilities in Windows OLE MS14-064 patched in November 2014. System installed the patch are safe. System without patch must install it. Without this patch every software utilizing MS Internet Explorer components including Internet Explorer itself can be vulnerable to specially crafted HTML page allowing code execution. WinRAR SFX module displays HTML in start dialog, so it is affected too, but components of Internet Explorer are used in a huge number of different tools, not just in WinRAR SFX archives.

MS14-064 patch is not available for Windows XP. Possible solution for XP users can involve disabling Active scripting in Internet Explorer Security Settings, installing an antivirus or even upgrading to a newer Windows, but it is beyond the scope of this article. It is important to realize that MS14-064 is a system wide vulnerability, affecting all applications utilizing Internet Explorer components. It is not something WinRAR specific.

This self-extracting issue does not affect WinRAR itself, because WinRAR does not display HTML code when extracting or opening archives, including self-extracting archives. Self-extracting archives, which are executable files, can be affected on unpatched systems, but unlike some other tools, security impact to self-extracting archives is negligible.

As we mentioned previously, this issue does not create any new risk factors for SFX archives. Being an executable file, SFX archive already can do everything what can be done with this MS14-064 vulnerability. SFX archive can run any local executable or download and run a remotely stored executable either utilizing SFX module "Setup" command or integrating the required code directly into SFX module. Even the entire SFX module can be replaced with malware by a malicious person. This is why it is safe to run SFX archives only if they are received from a trustworthy source.

Usual non-exe archives, such are .zip, .rar and other not .exe files, are not affected by this issue completely.

We would like to specially mention all those security sites and magazines blindly copying information about this issue. "Remote attack just by unzipping files", "500 million WinRAR users at risk", etc. etc. Many articles say that "We asked WinRAR to comment", but in fact we received only a single email from one responsible journalist, who contacted us himself. It is also interesting to see security experts claiming that this issue could lead to malicious file execution by anyone clicking on an archive containing the code. Running .exe file can lead to code execution. SFX module designed to execute extracted files can execute files. Surprise. Some of experts failed to realize that it is not related to usual non-exe archives and mentioned that all types of archive attachments are dangerous now. Some suggested to users to be careful with SFX archives until a patch by WinRAR is released. As if some magical patch allowing to safely run .exe files from untrustworthy sources could be possible. Some claimed that new issue is dangerous, because it allows to run files downloaded from Internet. Another surprise: you can specify a tool to download and run files in standard SFX "Setup" command and it is used by web installers for years. Also a web downloader can be placed just instead of SFX module code.

Lastly, I would like to note that R-73eN ( Rio Sherri ) of Infogen AL informed me that original code of that supposed SFX archive vulnerability published by Mohammad Reza is copied from R-73eN earlier code with insignificant modifications.

*Eugene Roshal, dev@rarlab.com,*
*RAR and WinRAR developer since 1993,*
*annoyed and irritated by million of articles*
*about Catastrophic WinRAR Vulnerability Going To Destroy Everything.*

*October 1st, 2015.*