Microsoft Patch Analysis for Exploitation

By Irongeek.com

Microsoft Patch Analysis for Exploitation

Stephen Sims
@Steph3nSims

BSidesCharm 2017
http://www.bsidescharm.com

Since the early 2000's Microsoft has distributed patches on the second Tuesday of each month. Bad guys, good guys, and many in-between compare the newly released patches to the unpatched version of the files to identify the security fixes. Many organizations take weeks to patch and the faster someone can reverse engineer the patches and get a working exploit written, the more valuable it is as an attack vector. Analysis also allows a researcher to identify common ways that Microsoft fixes bugs which can be used to find 0-days. Microsoft has recently moved to mandatory cumulative patches which introduces complexity in extracting patches for analysis. Join me in this presentation while I demonstrate the analysis of various patches and exploits, as well as the best-known method for modern patch extraction.

Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. Stephen has a MS in information assurance from Norwich University and is a course author and senior instructor for the SANS Institute. He is the author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISA, Immunity NOP, and many other certifications. In his spare time Stephen enjoys snowboarding and writing music.

Ett fel inträffade.

Det går inte att köra JavaScript.

Back to BSidesCharm 2017 list

Printable version of this article

15 most recent posts on Irongeek.com:

- OISF 2023 Videos
- OISF 2022
- Brian Rea (DeviantOllam Deviant) and Lesley Carhart (Hacks4Pancakes) continue their harassment of me
- OSInt, Doxing And Cyberstalking Page Updated
- OISF 2021 Videos
- BSides Cleveland 2021 Videos
- Who's Your Hacker
- BSides Tampa 2020 Videos
- Louisville Infosec 2019 Videos
- BSidesCT 2019 Video
- GrrCON 2019 Videos
- BSidesSTL 2019 Videos
- DerbyCon 9 Videos
- OISF 2019 Videos
- BSides Cleveland 2019 Videos