Security Newsletter

4 March 2019

Subscribe to this newsletter

Malspam Exploits WinRAR ACE Vulnerability to Install a Backdoor

Researchers have discovered a malspam campaign that is distributing a a malicious RAR archive that may be the first one to exploit the newly discovered WinRAR ACE vulnerability to install malware on a computer.

It allows a specially crafted ACE archive to extract a file to the Window Startup folder when it is extracted. This allows the executable to gain persistence and launch automatically when the user next logs in to Windows. As the developers of WinRAR no longer have access to the source code for the vulnerable UNACEV2.DLL library, instead of fixing the bug, they removed the DLL and ACE support from the latest version of WinRAR 5.70 beta 1. While this fixes the vulnerability, it also removes all ACE support from WinRAR.

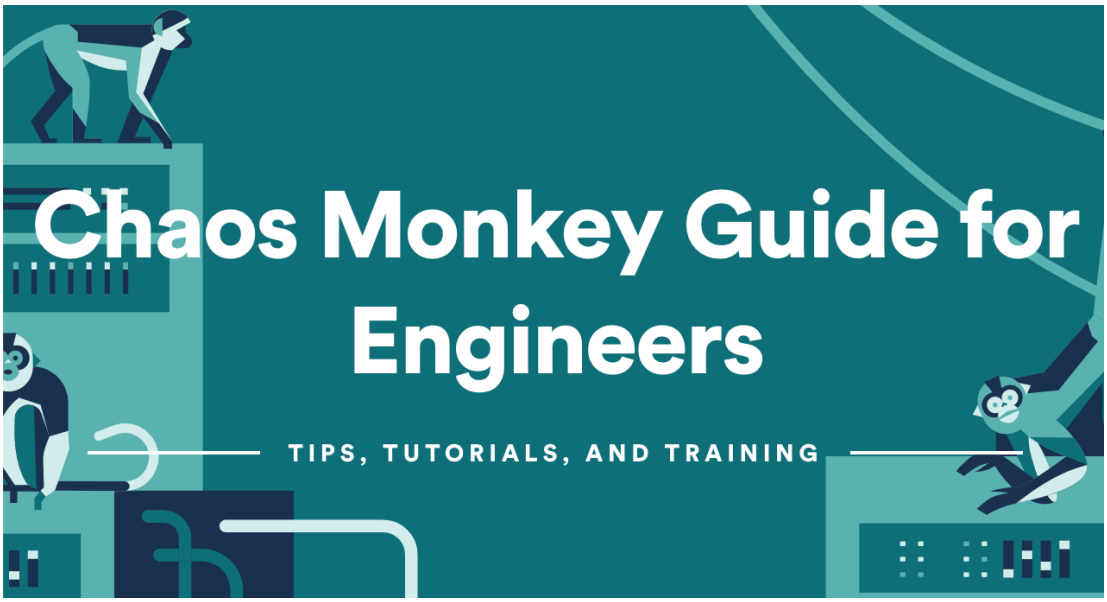
If UAC is running, when you attempt to extract the archive it will fail to place the malware in the C:\ProgramData folder due to lack of permissions. This will cause WinRAR to display an error stating "Access is denied" and "operation failed" as shown below.

If you are unable to upgrade for some reason, then you can use 0Patch's WinRAR micropatch to address this specific WinRAR bug. This micropatch will fix the vulnerability in all 32-bit and 64-bit versions of WinRAR versions using the UNACEV2.DLL since 2005.

Read More on BleepingComputer

Even More on SecurityWeek

Chaos Monkey Guide for Engineers

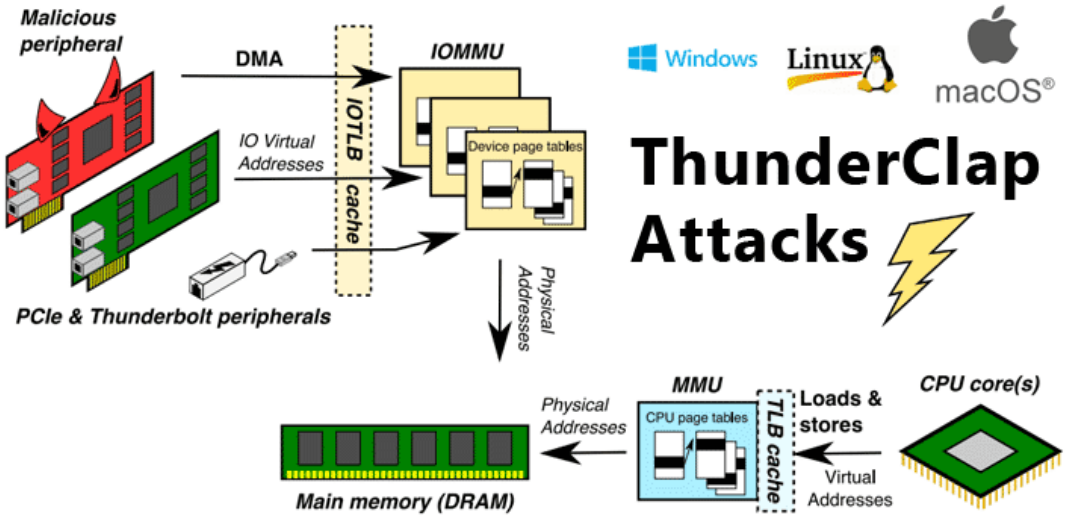


In 2010 Netflix announced the existence and success of their custom resiliency tool called Chaos Monkey. Netflix designed Chaos Monkey to test system stability by enforcing failures via the pseudo-random termination of instances and services within Netflix's architecture. Following their migration to the cloud, Netflix's service was newly reliant upon Amazon Web Services and needed a technology that could show them how their system responded when critical components of their production service infrastructure were taken down. Intentionally causing this single failure would suss out any weaknesses in their systems and guide them towards automated solutions that gracefully handle future failures of this sort.

In 2011, Netflix announced the evolution of Chaos Monkey with a series of additional tools known as The Simian Army. Inspired by the success of their original Chaos Monkey tool aimed at randomly disabling production instances and services, the engineering team developed additional "simians" built to cause other types of failure and induce abnormal system conditions. For example, the Latency Monkey tool introduces artificial delays in RESTful client-server communication, allowing the team at Netflix to simulate service unavailability without actually taking down said service. This guide will cover all the details of these tools in The Simian Army chapter.

Read More on Gremlin.com

New Flaws Re-Enable DMA Attacks On Wide Range of Modern Computers



Security researchers have discovered a new class of security vulnerabilities that impacts all major operating systems, including Microsoft Windows, Apple macOS, Linux, and FreeBSD, allowing attackers to bypass protection mechanisms introduced to defend against DMA attacks.

Known for years, Direct memory access (DMA)-based attacks let an attacker compromise a targeted computer in a matter of seconds by plugging-in a malicious hot plug device—such as an external network card, mouse, keyboard, printer, storage, and graphics card—into Thunderbolt 3 port or the latest USB-C port.

Researchers have reported their findings to all major hardware and operating system vendors, and most of them have already shipped substantial mitigation to address the Thunderclap vulnerabilities. Though not all software patches can entirely block DMA attacks, users are still advised to install available security updates to reduce the attack surface. According to the researchers, the best way to fully protect yourself is to disable the Thunderbolt ports on your machine, if applicable.

Read More on TheHackerNews

Even More on Thunderclap.io

More #News

- Top ten most popular docker images each contain at least 30 vulnerabilities
- Hackers Actively Exploiting Latest Drupal RCE Flaw Published Last Week
- Malvertising Attack Sneaks JavaScript Payload in Polyglot Images
- Microsoft font gives away forgery in bankruptcy case
- Less than one in 10 Americans take necessary steps to prevent identity theft

- Millions of utilities customers' passwords stored in plain text
- SHAREit App Vulnerabilities Allows Hackers to Bypass Android Device Authentication & Download Arbitrary Files Remotely
- Researchers break e-signatures in 22 common PDF viewers
- Researchers hide malware in benign apps with the help of speculative execution
- An Inside Look at a Level 4 Threat Hunting Program
- New Thai laws allow government to access information without warrants: Report
- Embracing DevSecOps: 5 Processes to Improve DevOps Security
- Retailers have become the top target for credential stuffing attacks
- AltFS Fileless File System Aims to Evade Detection by Security Software
- MageCart Group Evolves Tactics To Better Steal Your Credit Cards
- Vulnerability exposes location of thousands of malware C&C servers
- Android Gets FIDO2 Certification—Now Supports Secure Passwordless Logins
- Hackers Can Plant Backdoors on Bare Metal Cloud Servers: Researchers
- Most hackers just PowerShell through boxes now, leaving little in the way of footprints
- Mozilla fears encryption law could turn its employees into insider threats
- Digital extortionist offer high six-figure salaries to accomplices

#Patch Time!

- Cisco: Patch routers now against massive 9.8/10-severity security hole
- New Elevation of Privilege Vulnerability Found in Cisco WebEx Meetings
- Nvidia patches eight security flaws in graphics products
- Adobe patches the same critical Reader flaw twice in one week
- Google Chrome zero-day used in the wild to collect user data via PDF files
- Thunderclap
- Extracting a 19 Year Old Code Execution from WinRAR

#Tech and #Tools

- Google Cloud Platform (GCP) Bucket Enumeration and Privilege Escalation
- How To Secure A Linux Server
- Don't get clever with login forms
- Wireshark 3 Released with New Npcap Windows Packet Capturing Driver
- EdgeSpot detects PDF samples tracking users who use Google Chrome as local PDF viewer
- cut1
- Recovering the Master Password from a Locked Password Manager (1Password)
- How to break PDF Signatures
- Investigating WinRAR Code Execution Vulnerability (CVE-2018-20250) at Internet Scale
- CRXcavator: Chrome extension security analysis
- Eliminating opportunities for traffic hijacking
- Horizontal Privilege Escalation which can compromise all users on Quora
- Abusing Docker API | Socket
- Tales of a blue teamer: detecting powershell empire shenanigans with sysinternals
- Thinking outside of the password manager box

- cut1
- AltFS: The Alternative Fileless File System
- Top 10 web hacking techniques of 2018
- SHAREit Multiple Vulnerabilities Enable Unrestricted Access to Adjacent Devices' Files
- Jenkins - decrypting credentials.xml

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us