kindred

Security Newsletter

20 January 2020

Subscribe to this newsletter

Critical Windows Vulnerability Discovered by NSA

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
Proof-of-concept Exploits Released
for Microsoft-NSA Crypto Vulnerability

Yesterday's Microsoft Windows patches included a fix for a critical vulnerability in the system's crypto library. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source. The user would have no way of knowing the file was malicious, because the digital signature would appear to be from a trusted provider.

That's really bad, and you should all patch your system as soon as possible. This is a zero-day vulnerability, meaning that it was not detected in the wild before the patch was released. It was discovered by security researchers. Interestingly, it was discovered by NSA security researchers, and the NSA security advisory gives a lot more information about it than the Microsoft advisory does.

Two of the critical issues affect Windows Remote Desktop Gateway (RD Gateway), tracked as CVE-2020-0609 and CVE-2020-0610, that can be exploited by unauthenticated attackers to execute malicious code on targeted systems just by sending a specially crafted request via RDP. Fortunately, none of the flaws addressed this month by Microsoft were publicly disclosed or found being exploited in the wild.

Read More on Schneier on Security

Even More on TheHackerNews

More #News

- Lottery hacker gets 9 months for his £5 cut of the loot
- Tinder, Grindr Accused of Illegally Sharing User Data
- Microsoft Enables Security Defaults in Azure Active Directory
- 5 major US wireless carriers vulnerable to SIM swapping attacks
- Phishing for Apples, Bobbing for Links

- Powerful GPG collision attack spells the end for SHA-1
- Australia Bushfire Donors Affected by Credit Card Skimming Attack
- Google Chrome Aims to Make Browser User-Agents Obsolete
- Google tests biometric authentication for Android autofill
- Google will now accept your iPhone as an authentication key
- Facebook to notify users of third-party app logins
- These subject lines are the most clicked for phishing
- Announcing the Cloudflare Access App Launch
- Customer-Owned Bank Informs 100k of Breach Exposing Account Balance, PII
- Introducing Microsoft Application Inspector
- NSA Vulnerability Disclosure: Pros and Cons
- Password Shaming Isn't Productive – Passwords Are Scary Business
- Public Bug Bounty Program Launched for Kubernetes
- How to implement Multi-Factor Authentication (MFA)
- Equifax Ordered to Spend $1 Billion on Data Security Under Data Breach Settlement

#Patch Time!

- Patch Tuesday, January 2020 Edition
- Adobe's first 2020 security patch update fixes code execution vulnerabilities
- Citrix ADC CVE-2019-19781 Exploits Released, Fix Now!
- CISA Releases Test Tool for Citrix ADC CVE-2019-19781 Vulnerability
- Google Researchers Detail Critical iMessage Vulnerability
- Critical WordPress Plugin Bug Allows Admin Logins Without Password
- Windows 7: Microsoft Ceases Free Security Updates
- Oracle's January 2020 update patches 334 security flaws
- Microsoft Office January Security Updates Fix Code Execution Bugs

#Tech and #Tools

- lil-pwny: Auditing Active Directory passwords using multiprocessing in Python.
- What I Learned Watching All 44 AppSec Cali 2019 Talks
- Ban footguns: How to standardize how devs use dangerous aspects of your framework
- Practical tips for defending web applications in the age of agile/DevOps
- Security architecture anti-patterns
- Analyzing Magecart Malware – From Zero to Hero
- Creating Responders in The Hive
- Deceiving blue teams using anti-forensic techniques
- Encrypted Malware
- Fortinet FortiSIEM Hardcoded SSH Key
- An Empirical Study of Wireless Carrier Authentication for SIM Swaps

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. You can find all our open vacancies on our career page.

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 a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. 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 is an innovation driven company that builds on trust.

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