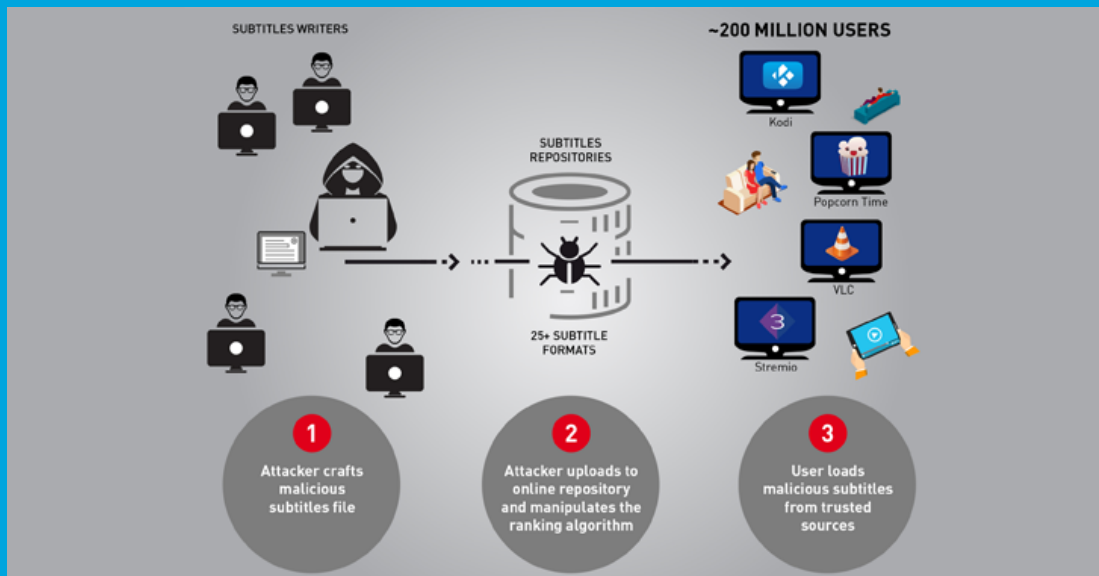




Security Newsletter

29 May 2017

Beware! Subtitle Files Can Hack Your Computer While You're Enjoying Movies



A team of researchers at Check Point has discovered vulnerabilities in four of the most popular media player applications, which can be exploited by hackers to hijack "any type of device via vulnerabilities; whether it is a PC, a smart TV, or a mobile device" with malicious codes inserted into the subtitle files.

The vulnerabilities reside in the way various media players process subtitle files and if exploited successfully, could put hundreds of millions of users at risk of getting hacked. As soon as the media player parses those malicious subtitle files before displaying the actual subtitles on your screen, the hackers are granted full control of your computer or Smart TV on which you ran those files.

Since text-based subtitles for movies and TV shows are created by writers and then uploaded to Internet stores, like OpenSubtitles and SubDB, hackers could also craft malicious text files for same TV shows and movies. The researchers believe that similar security vulnerabilities also exist in other streaming media players.

Check Point has already informed the developers of VLC, Kodi, Popcorn Time and Stremio applications about the recently discovered vulnerabilities. All of them have patched the flaws. **This is a good reminder of the importance to keep your whole system up to date, not just your operating system, you never know where the next attack will come from.**

[Read more](#)

[CheckPoint's Report](#)

Cloak and Dagger: Advanced device takeover attack on Android



Cloak and Dagger is a new class of potential attacks affecting Android devices. These attacks allow a malicious app to completely control the UI feedback loop and take over the device – without giving the user a chance to notice the malicious activity.

These attacks only require two permissions that, in case the app is installed from the Play Store, the user does not need to explicitly grant and for which she is not even notified. These attacks affect all recent versions of Android (including the latest version, Android 7.1.2), and they are yet to be fixed.

Abusing those permissions allows the attacker to perform several malicious tasks such as click-jacking, keylogging, stealing 2FA tokens, silent installation of ultra-permissive app, and more.

[Read More](#)

[Initial report](#)

Free course: The GDPR Attack Plan

What Constitutes "Offering Goods or Services"?



EU Office



EU Languages



EU Currencies



EU Domains

VARONIS SYSTEMS



The EU General Data Protection regulation will be law on May 25, 2018 - changing the landscape of regulated data protection law and the way that companies collect personal data. What are the requirements? Who will be affected? How does this help protect personal data? Does it only affect companies based in the EU? (hint: no.)


Troy Hunt released a free video course going through the roles of GPDR, understanding what Personal Data means, territorial scope, penalties and GDPR principles in action. You can access it through Varonis website, keep in mind can safely expect to be contacted by them if you use a corporate email.

[Read More](#)

[Course](#)

Samba exploit – not quite WannaCry for Linux, but patch anyway!

```
473  */
474  bool is_known_pipename(const char *pipename, struct ndr_syntax_id *syntax)
475  {
476      NTSTATUS status;
477
478  > if (!lp_disable_spoolss() && strequal(pipename, "spoolss")) {
479      DEBUG(10, ("refusing spoolss access\n"));
480      return false;
481  }
482
483  if (v_get_pipe_interface_by_name(pipename, syntax)) {
484      return true;
485  }
486
487  status = probe_module("rpc", pipename);
488  if (NT_SUCCESS(status)) {
489      DEBUG(10, ("is_known_pipename: %s unknown\n", pipename));
490      return false;
491  }
492  DEBUG(10, ("is_known_pipename: %s loaded dynamically\n", pipename));
493
494  /*
495   * Scan the list again for the interface id
496   */
497  if (rpc_srv_get_pipe_interface_by_cli_name(pipename, syntax)) {
```



SAMBACRY

CVE-2017-7494

Samba is open-source software (re-implementation of SMB networking protocol) that runs on the majority of operating systems available today, including Windows, Linux, UNIX, IBM System 390, and OpenVMS. A 7-year-old critical remote code execution vulnerability has been discovered in Samba networking software that could allow a remote attacker to take control of an affected Linux and Unix machines.

All versions of Samba from 3.5.0 onwards are vulnerable to a remote code execution vulnerability (CVE-2017-7494), allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it. Samba 3.5.0 was released on March 1, 2010. Some experts are saying it is "Linux version of EternalBlue," used by the WannaCry ransomware.

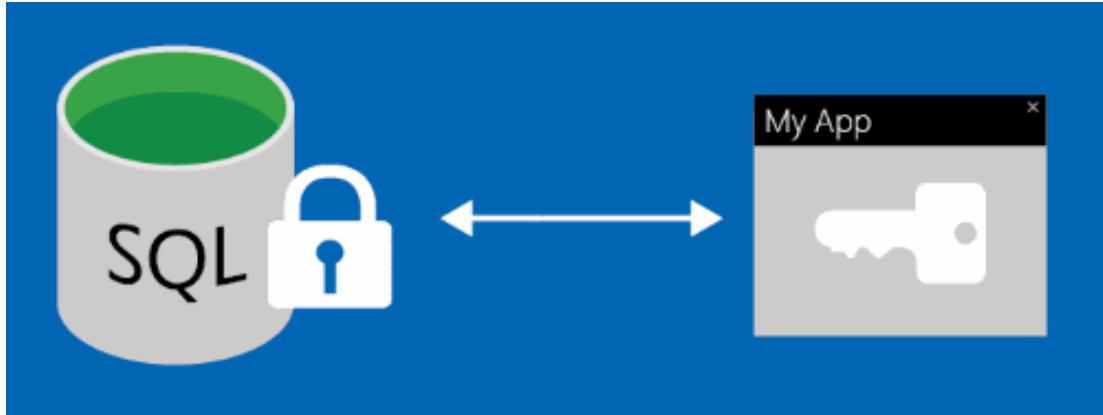
The vulnerability is hell easy to exploit. Just one line of code is required to execute malicious code on the affected system (*simple.create_pipe("/path/to/target.so")*). The Samba exploit has already been ported to Metasploit, a penetration testing framework, enabling researchers as well as hackers to exploit this flaw easily.

The maintainers of Samba has already patched the issue in their new versions Samba versions 4.6.4/4.5.10/4.4.14, and are urging those using a vulnerable version of Samba to install the patch as soon as possible. If you can not upgrade to the latest versions of Samba, you can work around the vulnerability by adding *"nt pipe support = no"* to your Samba configuration file *smb.conf*. Samba maintainers have also provided patches for older and unsupported versions of Samba.

[Read More](#)

[CVE](#)

Building Searchable Encrypted Databases with PHP and SQL



This question shows up from time to time in open source encryption libraries' bug trackers: How do we securely encrypt database fields but still use these fields in search queries?

Paragon's secure solution is rather straightforward, but the path between most teams asking that question and discovering our straightforward solution is fraught with peril: bad designs, academic research projects, misleading marketing, and poor threat modeling.

In order to store encrypted information and still use the plaintext in SELECT queries, we're going to follow a strategy we call blind indexing. The general idea is to store a keyed hash (e.g. HMAC) of the plaintext in a separate column. It is important that the blind index key be distinct from the encryption key and unknown to the database server..

[Read More](#)

Security Firm Releases Windows XP Patch for NSA Exploit ESTEEMAUDIT



Cyber-security firm enSilo has released a patch for Windows XP and Windows Server 2003 that will protect against attacks via ESTEEMAUDIT, a hacking tool dumped online by the Shadow Brokers last month, and allegedly developed by the NSA. At the technical level, ESTEEMAUDIT is a zero-day in the RDP protocol used by Windows to open desktop sessions on remote computers.

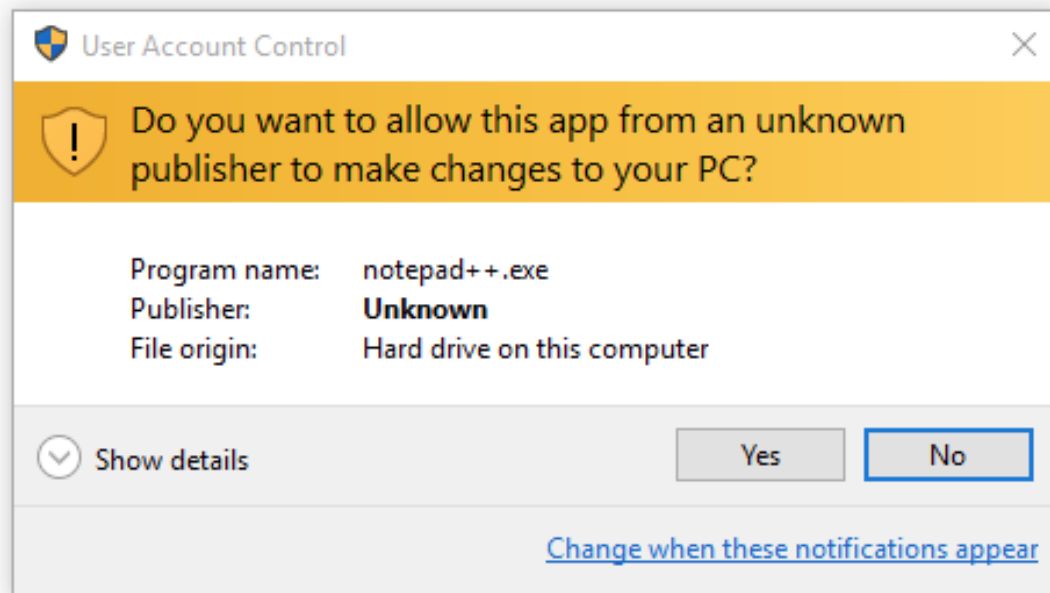
After the Shadow Brokers dumped a collection of NSA hacking tools on April 14, a day later, Microsoft announced that its engineers had secretly patched Windows against most exploits a month earlier, in March. ESTEEMAUDIT is one of the exploits that didn't receive a patch, along with ENGLISHMANSIDENTIST and EXPLODINGCAN. This is because ESTEEMAUDIT only works on Windows XP and Windows 2003, two operating system that Microsoft stopped supporting in 2014, and 2015, respectively.

EnSilo researchers developed a patch for ESTEEMAUDIT. The security company says the patch – which can be downloaded from here – works on Windows XP SP3 x86, Windows XP SP3 x64, and Windows Server 2003 R2. Besides applying the enSilo patch, users can disable RDP as an alternative method of protecting their systems.

[Read more](#)

[Download page](#)

Windows AppLocker protection and UAC are vulnerable to new bypass techniques



AppLocker is a security service introduced with Windows 7 and Windows Server 2008 R2 that allows system administrators to restrict access to Windows applications based on a rule-based system. An attacker or a rogue employee can create and register custom control panel items through registry and use these files to bypass the Windows AppLocker security feature.

This bypass technique is possible because both registry and Control Panel are Microsoft-signed binaries, allowed by AppLocker by default. While blocking access to utilities like reg, regedit, and the Control Panel is one alternative, the attack can also be mitigated, at the cost of performance, by enabling the 'DLL Rule Collection' under the AppLocker 'Advanced' tab.

User Account Control (UAC) is a feature introduced with Microsoft's Windows Vista which aims to improve the security by limiting applications to standard user privileges until an administrator authorizes an increase or elevation. A new bypass method has been discovered by Christian B., a German student currently working on his master's thesis in cybersecurity.

Despite this, Christian's UAC bypass is not universal, as users need to be part of the operating system's administrator group. While on paper this sounds like a huge restriction, this isn't actually such a big issue on Windows, where most users utilize an admin-level account to manage their PCs.

Applocker bypass

UAC bypass

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 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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.