kindred

Security Newsletter

19 July 2017

Critical Flaws Found in Windows NTLM Security Protocol – Patch Now

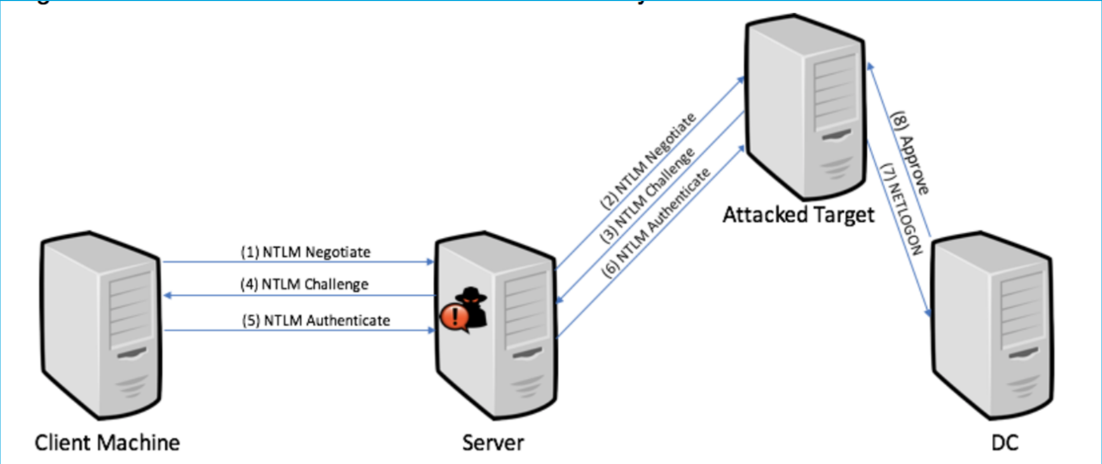


Figure 1 - NTLM relay basic flow

The Preempt research team discovered and reported two Microsoft NT LAN Manager (NTLM) vulnerabilities. These issues are particularly significant as they can potentially allow an attacker to create new domain administrator accounts even when best-practice controls such as LDAP server signing and RDP restricted admin mode are enabled.

NTLM is a suite of Microsoft security protocols that enables authentication, integrity, and confidentiality for users. A video demonstration of the two vulnerabilities can be seen here.

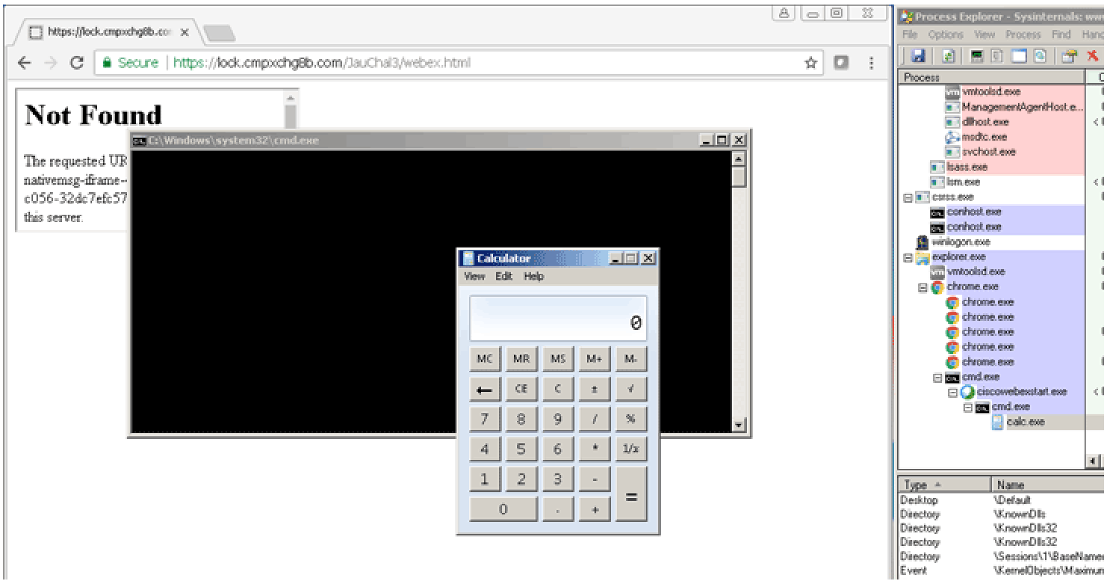
Microsoft acknowledged both issues. For the first, a CVE has been issued (CVE-2017-8563) and a fix has been released. **For the second, Microsoft, claimed it is a “known issue” and recommend configuring network to be safe from any sort of NTLM relay.**

The bottom line: NTLM is very risky as it puts you at risk of credential forwarding and password cracking. If you can, you should avoid using it in your network and you’ll be a lot safer. If it is not feasible for your organization, you'll find recommendations at the end of the article to mitigate the risks.

Read More

CVE-2017-8563

Critical RCE Vulnerability Found in Cisco WebEx Extensions, Again — Patch Now!



Not Found

The requested UR
nativemsg-iframe-
c056-32dc7efc57
this server.

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\KnownDlls32
Directory	\KnownDlls32
Directory	\Sessions\1\BaseName
Event	\KernelObjects\Maximun

A highly critical vulnerability has been discovered in the Cisco Systems' WebEx browser extension for Chrome and Firefox, for the second time in this year, which could allow attackers to remotely execute malicious code on a victim's computer.

Discovered by Tavis Ormandy of Google Project Zero and Cris Neckar of Divergent Security, the remote code execution flaw (CVE-2017-6753) is due to a designing defect in the WebEx browser extension. **To exploit the vulnerability, all an attacker need to do is trick victims into visiting a web page containing specially crafted malicious code through the browser with affected extension installed.**

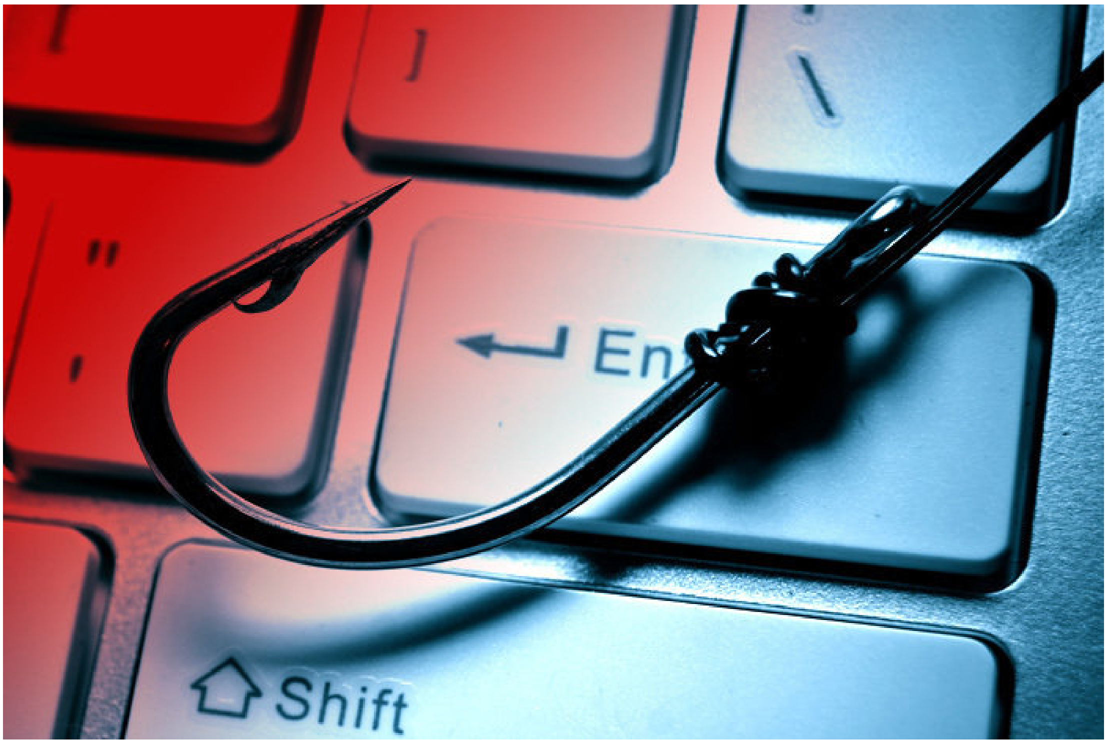
Cisco has already patched the vulnerability and released "Cisco WebEx Extension 1.0.12" update for Chrome and Firefox browsers that address this issue, though "there are no workarounds that address this vulnerability."

In general, users are always recommended to run all software as a non-privileged user in an effort to diminish the effects of a successful attack.

Read More

Google Zero bug report

Top 10 phishing email subject lines that launch ransomware



Ninety-one percent of attacks by cyber criminals start through phishing, according to email security provider Mimecast. The Cisco 2017 Annual Cybersecurity Report states that ransomware is growing at a yearly rate of 350 percent.

Want to protect your organization from the next ransomware outbreak? Give this list of the top 10 global most-clicked phishing email subject lines for Q2 2017, recently published by KnowBe4, to your employees.

Security Alert – *21%*; Revised Vacation & Sick Time Policy – *14%*; UPS Label Delivery 1ZBE312TNY00015011 – *10%*; BREAKING: United Airlines Passenger Dies from Brain Hemorrhage – VIDEO – *10%*; A Delivery Attempt was made – *10%*; All Employees: Update your Healthcare Info – *9%*; Change of Password Required Immediately – *8%*; Password Check Required Immediately – *7%*; Unusual sign-in activity – *6%*; Urgent Action Required – *6%*

Read More

Insider scammed $14.3m lottery ‘win’ by manipulating random number generator

One of the biggest lottery scams in the history of the US is coming to a close as the mastermind behind the operation has pleaded guilty in an Iowa court, at the end of last month.

Eddie Tipton, 54, admitted to creating malware in the form of a DLL file, which he loaded on the secure computers of the Multi-State Lottery Association (MSLA), a company that runs lotteries in 33 states, but also in the District of Columbia, Puerto Rico and the U.S. Virgin Islands.

Tipton was able to do this because he served as the company's computer information security director in its Urbandale, Iowa headquarters, and was one of the five persons that had access to those computers, situated in the "draw room."

Read More

Even More

API-Security-Checklist

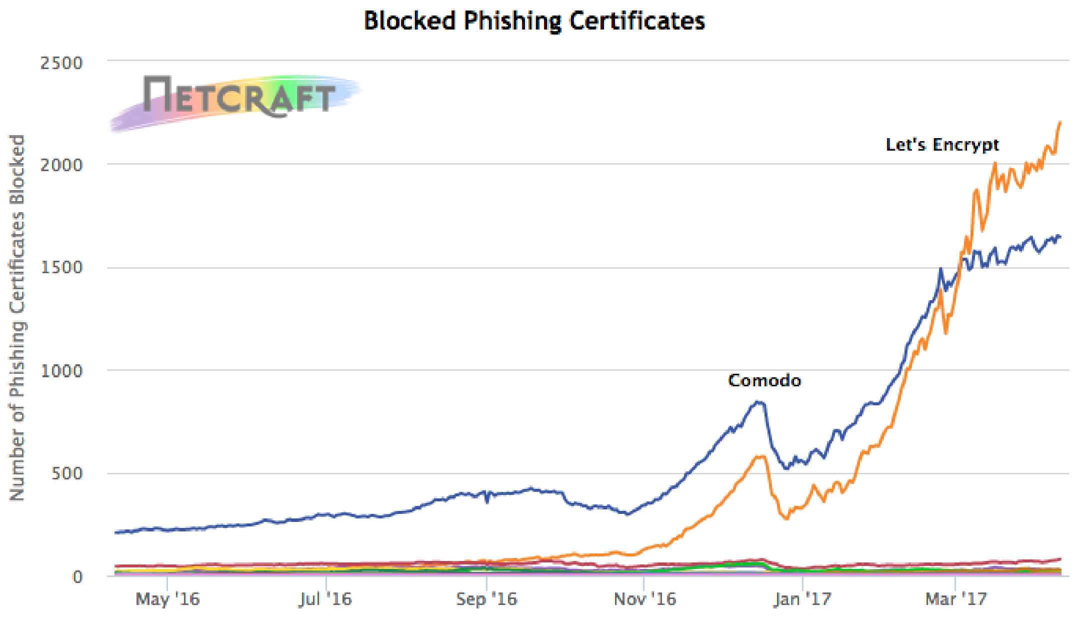
Checklist of the most important security countermeasures when designing, testing, and releasing your API.

While some items are debatable, for example, a lot of people in infosec do have a grip against JWT, others try to promotes alternatives such as Macaroons, that can be attenuated and delegated in ways that JWTs can not, or things like Fernet.

Otherwise it seems like a very good starting point when assessing the security of an existing API or designing a new one.

Read More

On The (Perceived) Value of EV Certs, Commercial CAs, Phishing and Let's Encrypt



There are two important things happening here: Any page including a form element loaded over a non-secure connection will display "Not secure" (at least once you click on it). Any non-secure page at all loaded in Incognito mode will also display "Not secure" (and it'll do it all the time)

A cornerstone of the anti-Let's Encrypt movement has been the use of their certificates for malicious purposes, particularly in phishing campaigns. Certs are valuable for building trust in victims because the presence of HTTPS provides increased visual assurance of the safety of the site. You'll see the word "Secure" next to the address bar in Chrome on the desktop, a padlock next to the URL in Safari on iOS and other similar implementations in different clients

One really important part of the narrative here is that a CA issuing certs which are then used for malicious purposes in no way jeopardises the viability of that CA for other customers. But regardless of the CA, the ready availability of these certs that can be used for malicious purposes clearly poses a challenge due to user-conditioning to recognise the padlock icon as a sign of trustworthiness. HTTPS & SSL doesn't mean "trust this." It means "this is private." You may be having a private conversation with bad guys.

Read More

Node JS Denial of Service critical vulnerability

A bug exists in Node.js, all versions of v0.12.x through to v5.x inclusive, whereby an external attacker can cause a denial of service. The severity of this issue is high (7.5/10) and users of the affected versions should plan to upgrade when a fix is made available.

Versions 0.12.x, 4.x, including LTS Argon and 5.x of Node.js are vulnerable. Versions 0.10.x of Node.js are not affected.

An additional bug exists in Node.js, all versions of v4.x and v5.x, whereby an attacker may be able to trigger an out-of-bounds access and/or denial of service if user-supplied JavaScript can be executed by an application. The severity of this issue is considered medium for Node.js users (4.4/10), but only under circumstances where an attacker may cause user-supplied JavaScript to be executed within a Node.js application. Fixes will be shipped for the v4.x and v5.x release lines along with fixes for CVE-2015-8027.

Read More

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.