kindred

Security Newsletter

25 September 2017

Subscribe to this newsletter

Warning: CCleaner Hacked to Distribute Malware; Over 2.3 Million Users Infected

If you have downloaded or updated CCleaner application on your computer between August 15 and September 12 of this year from its official website, then pay attention—your computer has been compromised.

Earlier this month, researchers found CCleaner and CCleaner Cloud were being illegally altered before they were released to the public. The download for CCleaner v5.33 was accompanied by a multi-stage malware payload, signed using a valid digital signature issued to Piriform.

This incident is yet another example of supply chain attack. Earlier this year, update servers of a Ukrainian company called MeDoc were also compromised in the same way to distribute the Petya ransomware, which wreaked havoc worldwide.

During the analysis of the hackers' command-and-control (C2) server to which the malicious CCleaner versions connected, security researchers from Cisco's Talos Group found evidence of a second payload (GeeSetup_x86.dll, a lightweight backdoor module) that was delivered to a specific list of computers based on local domain names. The target companies included: Google, Microsoft, Cisco, Intel, Samsung, Sony, HTC, Linksys, D-Link, Akamai, VMware

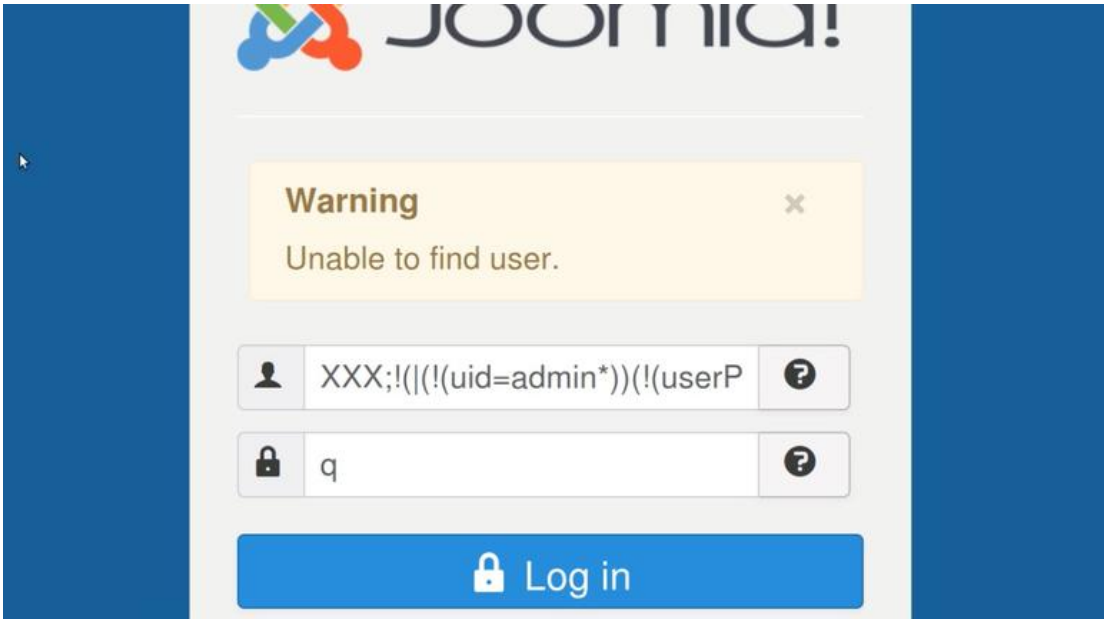
Piriform estimated that up to 3 percent of its users (up to 2.27 million people) were affected by the malicious installation. Affected users are strongly recommended to update their CCleaner software to version 5.34 or higher, in order to protect their computers from being compromised.

Read More

Avast-Owned Piriform Releases CCleaner Security Update

CCleaner Malware Infects Big Tech Companies With Second Backdoor

Joomla patches eight-year-old critical CMS bug



Joomla has patched a critical bug which could be used to steal account information and fully compromise website domains. They provider issued a security advisory detailing the flaw, which is found in the LDAP authentication plugin.

Joomla considers the bug a "medium" severity issue, but according to researchers from RIPS Technologies, the problem is closer to a critical status. Through the flaw, CVE-2017-14596, a remote attacker is able to extract authentication credentials from the LDAP server, including the super user username and password, as long as Joomla is configured to use LDAP for authentication.

The attacker does not need any privileges to exploit the bug, which has been present in the plugin for the past eight years. It is not known if the issue has been exploited in the wild. After the vulnerability was disclosed to the Joomla team and confirmed in July, a fix has been released through the latest Joomla release, version 3.8.

Read More

All That's Needed To Hack Gmail And Rob Bitcoin: A Name And A Phone Number

Hackers have proven just how urgently a gaping flaw in the global telecoms network, affecting what's known as Signalling System No. 7 (SS7), needs to be fixed. In a video demonstration, shown to Forbes ahead of publication today, benevolent hackers from Positive Technologies were able to take control of a Coinbase bitcoin wallet and start pilfering funds via the SS7 flaws.

In their attack, the Positive researchers first went to Gmail, using Google's service to find an email account with just a phone number. Once the email account was identified, the hackers initiated a password reset process, asking one-time authorization codes to be sent to the victim's phone. By exploiting SS7 weaknesses they were able to intercept text messages containing those codes, allowing them to choose a new password and take control of the Gmail account. They could then simply head to the Coinbase website and do another password reset using the email they'd compromised.

The biggest barrier, perhaps, to such attacks is acquiring access to the SS7 network in the first place. Criminals have, on at least one occasion, used SS7 vulnerabilities to carry out an attack. That occurred in Germany this year, when crooks were able to use the same methods as the Positive researchers, but to pilfer funds from bank accounts of O2-Telefonica customers.

While the world waits for telecoms companies to act, users could also stop using SMS for two-factor authentication.

Read More

Even More

With Forseti, Spotify and Google release GCP security tools to open source community

Spotify and Google Cloud worked together to develop innovative security tools that help organizations protect GCP (Google Cloud Platform) projects, and have made them available in an open source community called Forseti Security. Forseti is now open to all GCP users!

Forseti is an open source toolkit designed to help give security teams the confidence and peace of mind that they have the appropriate security controls in place across GCP. Today, Forseti features a number of useful security tools:

- Inventory: provides visibility into existing GCP resources
- Scanner: validates access control policies across GCP resources
- Enforcer: removes unwanted access to GCP resources
- Explain: analyzes who has what access to GCP resources

We had the opportunity to see in details the tool's potential through a great talk by Carly Schneider at SEC-T. Needless to say this is really promising!

Read More

Forseti homepage

Critical VMware vulnerability bypassing guest isolation (VMEscape), patch now

On September 15, VMware issued a notice that some versions of ESXi, Workstation and Fusion are affected by an out-of-bounds write vulnerability.

The out-of-bounds write vulnerability in VMware's products allows guests to break out of their isolation—an attacker could escape the confines of a virtual machine and execute malicious code on the machine the VM is running on.

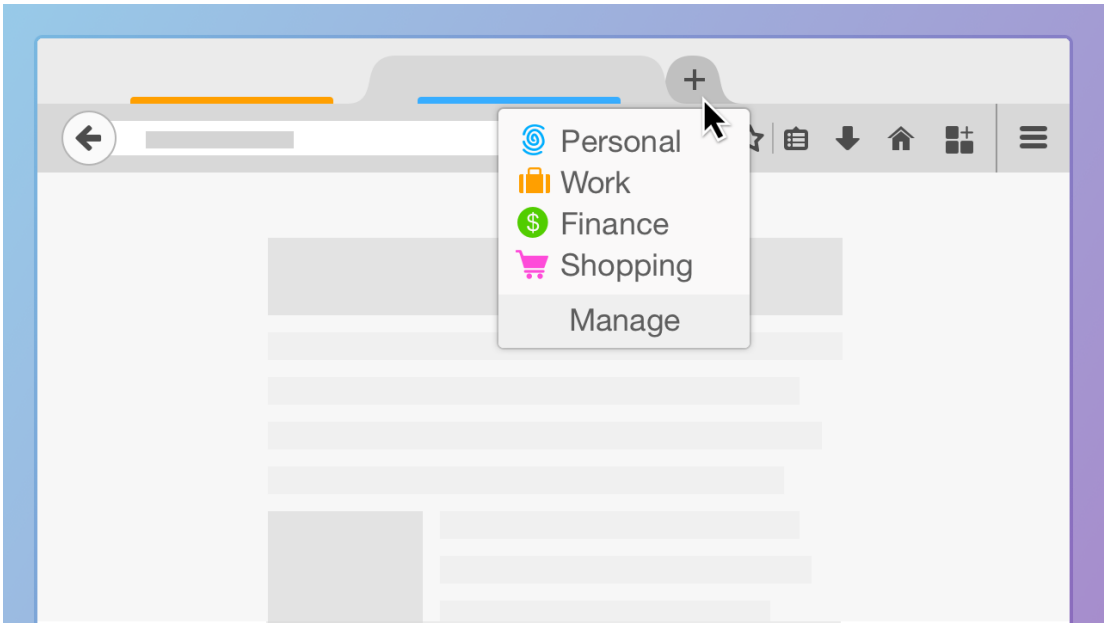
The impact of this vulnerability is potentially quite high, which is why VMware rates this vulnerability as critical; however, the Zero Day Initiative, which worked with the two researchers who discovered this issue to disclose it to VMware, gives this vulnerability only a medium score of 6.2. The nuance behind ZDI's reasoning is that while the impact is potentially high, this is not an easy vulnerability to exploit.

Thankfully VMware issued a fix for this vulnerability (CVE-2017-4924 for those keeping track at home), so the standard advice of "patch ASAP" applies. ESXi version 6.5, Workstation 12.x, and Fusion 8.x on OSX are all vulnerable to this bug, so update as soon as you can if you haven't yet.

Read More

CVE-2017-4924

Put your multiple online personalities in Firefox Multi-Account Containers



Maybe you've got two Gmail or Instagram or Twitter or Facebook accounts (or a few more than that). Maybe you want to keep your bank's website farther away from your Pinterest board. Maybe you just like to keep everything very, very organized. Firefox got an extension for you!

The Firefox Multi-Account Containers extension lets you carve out a separate box for each of your online lives. Each Container stores cookies separately, so you can log into the same site with different accounts and online trackers can't easily connect the browsing.

Custom labels and color-coded tabs help keep your different activities or personas separate. Exciting, right? Contain yourself! Install the Firefox Multi-Account Containers extension today and be who you want to be.

Read More

Download the extension

Apache “Optionsbleed” vulnerability – what you need to know

Remember Heartbleed? The Heartbleed vulnerability was that you could sneakily tell the server to reply with more data than you originally sent in, and instead of ignoring your malformed request, the server would send back your data…plus whatever was lying around nearby in memory, even if that was personal data or private data such as encryption keys from the web server itself.

Well, something similar has happened again. This time, the bug isn’t in OpenSSL, but in a program called httpd, probably better known as the Apache Web Server, and officially called the Apache HTTP Server Project. The vulnerability has been dubbed OptionsBleed, because the bug is triggered by making HTTP OPTION requests.

Apache servers can be configured by putting files called .htaccess into the directory tree of content that is stored on the server. Each .htaccess file sets configuration options for the directory it’s in and all the others below it. One of the settings you can configure in your .htaccess files allows to limit the available OPTIONS in the current directory tree. But here’s the thing: if any of the HTTP methods you configure in a directive are inapplicable, for example because you typed DELLETE instead of DELETE, the “Optionsbleed” bug is triggered.

The good news is that the side-effects of the bug don’t seem to show up often, given that it requires the coincidence of an incorrectly-configured .htaccess file and an unluckily-timed OPTIONS request. There is no official patch yet, we suggest you visit all your .htaccess files looking for settings that aren’t applicable (or are mis-spelled).

Read More

Recommendations

Cutting room floor

- How I hacked hundreds of companies through their helpdesk
- The Pirate Bay Website Runs a Cryptocurrency Miner (Updated)
- iOS 11's Control Center may say Bluetooth, Wi-Fi are off, but that's just not true
- Attackers Take Over WordPress, Joomla, JBoss Servers to Mine Monero
- Equifax has been sending customers to a fake phishing site for weeks
- Google Experiment Tests Top 5 Browsers, Finds Safari Riddled With Security Bugs
- Experian Site Can Give Anyone Your Credit Freeze PIN
- Kali Linux 2017.2 Release

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.

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