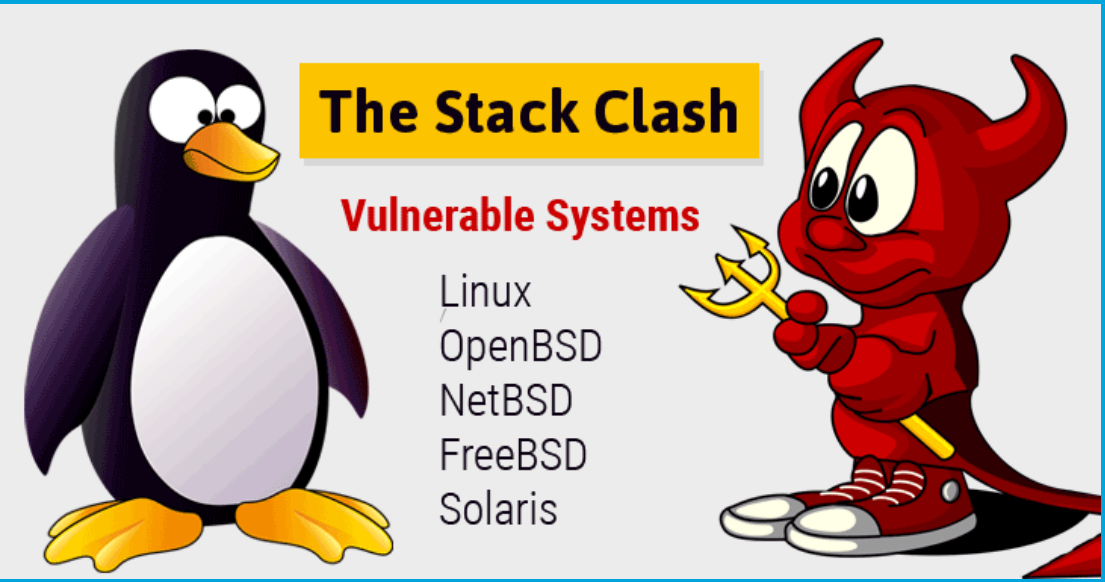
Security Newsletter

27 June 2017

Stack Clash: A Decade Old Unix/Linux/BSD Root Privilege-Escalation Bug Discovered



Security researchers have discovered more than a decade-old vulnerability in several Unix-based operating systems — including Linux, OpenBSD, NetBSD, FreeBSD and Solaris — which can be exploited by attackers to escalate their privileges to root, potentially leading to a full system takeover.

Each program uses a special memory region called the stack, which is used to store short-term data. It expands and contracts automatically during the execution of any program. A malicious program can attempt to use more memory space than available on the stack, which could overflow the memory, causing it to collide or clash with nearby memory regions and overwrite their content.

Moreover, the Stack Clash exploit can also bypass the stack guard-page, a memory management protection introduced in 2010, after this issue was exploited in 2005 and 2010. The Stack Clash vulnerability requires local access to the vulnerable system for exploitation. Attackers can also combine the Stack Clash bug with other critical vulnerabilities, like the Sudo vulnerability recently patched, and then run arbitrary code with the highest privileges, said Qualys researchers.

Many affected vendors have already issued security patches for the bug, so users and administrators are advised to install patches a soon as possible. It is also recommended to recompile all userland code (ld.so, libraries, binaries) with the –fstack-check feature. This would prevent the stack pointer from moving into another memory region without accessing the stack guard-page and would kill Stack Clash dead.

Read More

Technical Advisory

Deep Root: what can we learn from the GOP's data leak?

The US Republicans political party's data analytic contractor, Deep Root Analytics, had stored 25 terabytes (TB) of data in the cloud, of which 1.1TB were available for harvesting by anyone who found the links.

secure data in the cloud is only secure if you secure it. Few take the time to ensure that the data they heave by the terabytes into the cloud are adequately protected. Deep Root used Amazon Web Services (AWS) for storage.

According to a survey by Threat Stack, 73% of companies (out of 200 companies surveyed) had security misconfigurations within AWS that would leave "SSH wide open to the internet". The same survey found that 62% of companies were not using multifactor authentication for users accessing AWS data stores.

Read More

Euro MPs back end-to-end encryption for all citizens

A European Parliament committee is proposing that end-to-end encryption be enforced on all forms of digital communications to protect citizens. The draft legislation seeks to protect sensitive personal data from hacking and government surveillance. A ban on "backdoors" into encrypted messaging apps like WhatsApp and Telegram is also being considered.

During the UK's recent election campaign, the Conservative Party said that tech firms should provide the authorities "access to information as required" to help combat online radicalisation. However, cyber-security experts warn that criminals can still find a way to protect their communications, even if end-to-end encryption is banned.

End-to-end encryption means the company providing the service does not have access to the key, meaning it cannot "listen in" to what is being shared - giving the sender and recipient added confidence in the privacy of their conversation.

Read More

Is Continuing to Patch Windows XP a Mistake?

Recently, Microsoft issued a security patch for Windows XP, a 16-year-old operating system that Microsoft officially no longer supports. Last month, Microsoft issued a Windows XP patch for the vulnerability used in WannaCry.

The company had three ways it could respond. It could have done nothing -- stuck to its guns, maintained that the end of support means the end of support, and encouraged people to move to a different platform. It could also have relented entirely, extended Windows XP's support life cycle for another few years and waited for attrition to shrink Windows XP's userbase to irrelevant levels. Or it could have claimed that this case is somehow "special," releasing a patch while still claiming that Windows XP isn't supported.

None of these options is perfect. A hard-line approach to the end-of-life means that there are people being exploited that Microsoft refuses to help. A complete about-turn means that Windows XP will take even longer to flush out of the market, making it a continued headache for developers and administrators alike.

Read More

New GhostHook Attack Bypasses Windows 10 PatchGuard Protections

PatchGuard, known under its official name of Kernel Patch Protection (KPP), is a security feature for Windows 64-bit editions that prevents third-party code from patching the Windows kernel with additional routines. Microsoft introduced PatchGuard in 2005, starting with Windows XP, and the feature has prevented most rootkits from working on 64-bit editions.

Security researchers from CyberArk published research on a new technique named GhostHook that successfully bypasses PatchGuard using a feature of Intel CPUs, which allows an attacker to plant rootkits on systems previously thought to be impregnable.

Microsoft declined to issue a security update. Microsoft said it might patch the issue during its regular bug fixing cycle, but would not treat GhostHook as a security flaw. Microsoft justified its decision by saying that an attacker needs to have kernel-level access on an infected machine to perform a GhostHook attack. An attacker with kernel-level rights could perform many other malicious actions, and users should focus on preventing an attacker from gaining this much level of access in the first place.

The real problem is that attackers have a technique at their disposal to implant rootkits on platforms they did not have access in past years. Currently, 64-bit malware makes up less than 1% of the entire malware landscape, and PatchGuard was one of the reasons that helped keep 64-bit versions secure and harder to infect.

Read More

Technical advisory

Critical RCE Flaw Found in OpenVPN that Escaped Two Recent Security Audits

OpenVPN is one of the most popular and widely used open source VPN software solutions mostly used for various connectivity needs, but it is especially popular for anonymous and private access to the Internet. A security researcher has found four vulnerabilities, including a critical remote code execution bug, in OpenVPN, those were not even caught in the two big security audits of the open source VPN software this year.

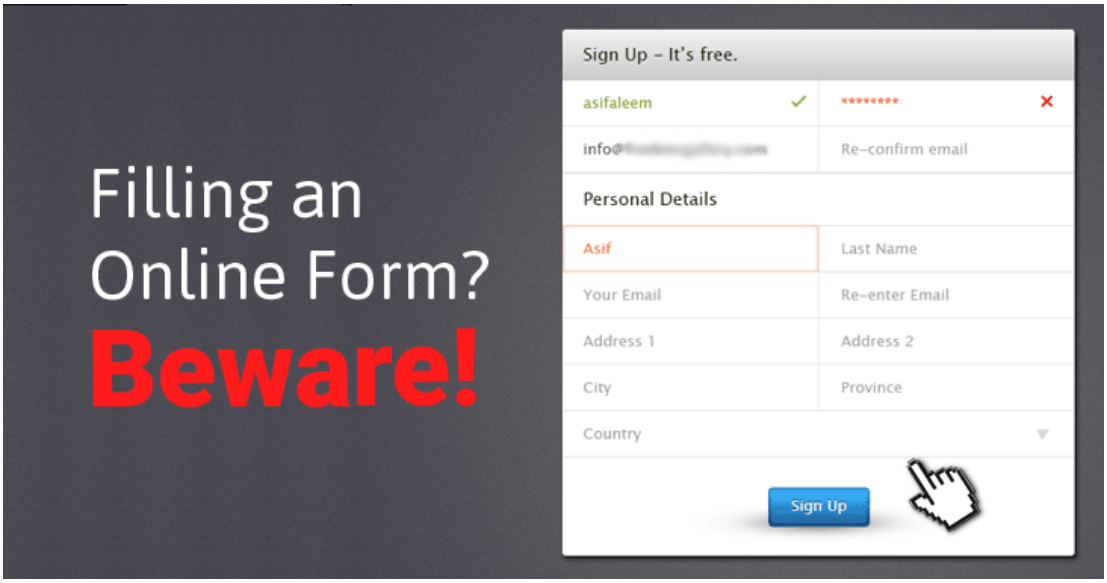
Researcher Guido Vranken of Netherlands exclusively used a fuzzer and recently discovered four security holes in OpenVPN that escaped both the security audits. Three of the four flaws the researcher discovered are server-side, two of which cause servers to crash, while the remaining is a client-side bug that could allow an attacker to steal a password to gain access to the proxy.

Vranken responsibly disclosed all the vulnerabilities he discovered to the OpenVPN team in May and June and the team has already patched the issues in its latest version of the VPN software. While there is no proof of any of the vulnerabilities had been publicly exploited, users are strongly advised to update their installations to OpenVPN versions 2.4.3 or 2.3.17 as soon as possible in order to be on the safer side.

Read More

Technical advisory

WebSites Found Collecting Data from Online Forms Even Before You Click Submit



'Do I really need to give this website so much about me?' That's exactly what we usually think after filling but before submitting a web form online asking for my personal details to continue. I am sure most of you would either close the whole tab or would edit already typed details (or filled up by browser's auto-fill feature) before clicking 'Submit' — Isn't it?

But closing the tab or editing your information hardly makes any difference because as soon as you have typed or auto-filled anything into the online form, the website captures it automatically in the background using JavaScript, even if you haven't clicked the Submit button. During an investigation, Gizmodo has discovered that code from NaviStone used by hundreds of websites, invisibly grabs each piece of information as you fill it out in a web form before you could hit 'Send' or 'Submit.'

In order to protect yourself from such websites collecting your data without your consent, you should consider disabling auto-fill form feature, which is turned on by default, in your browser, password manager or extension settings.

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.