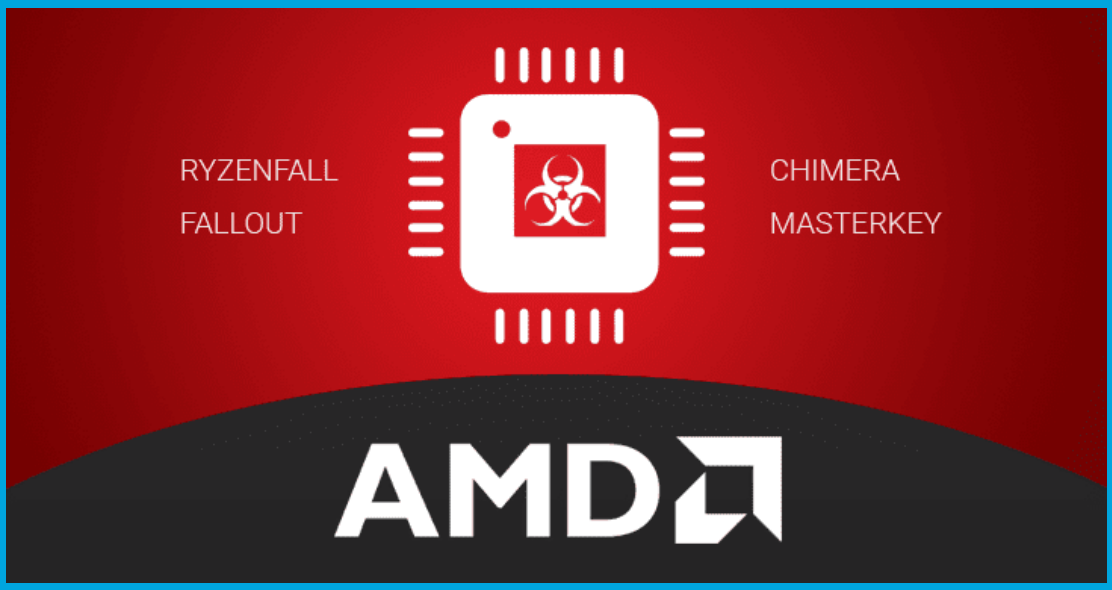
kindred

Security Newsletter

19 March 2018

Subscribe to this newsletter

Featured



Security researchers claimed to have discovered 13 critical Spectre/Meltdown-like vulnerabilities throughout AMD's Ryzen and EPYC lines of processors that could allow attackers to access sensitive data, install persistent malware inside the chip, and gain full access to the compromised systems. All these vulnerabilities reside in the secure part of the AMD's Zen architecture processors and chipsets—typically where device stores sensitive information such as passwords and encryption keys and makes sure nothing malicious is running when you start your PC.

The alleged vulnerabilities are categorized into four classes—RYZENFALL, FALLOUT, CHIMERA, and MASTERKEY—and threaten wide-range of servers, workstations, and laptops running vulnerable AMD Ryzen, Ryzen Pro, Ryzen Mobile or EPYC processors. Discovered by a team of researchers at Israel-based CTS-Labs, newly disclosed unpatched vulnerabilities defeat AMD's Secure Encrypted Virtualization (SEV) technology and could allow attackers to bypass Microsoft Windows Credential Guard to steal network credentials.

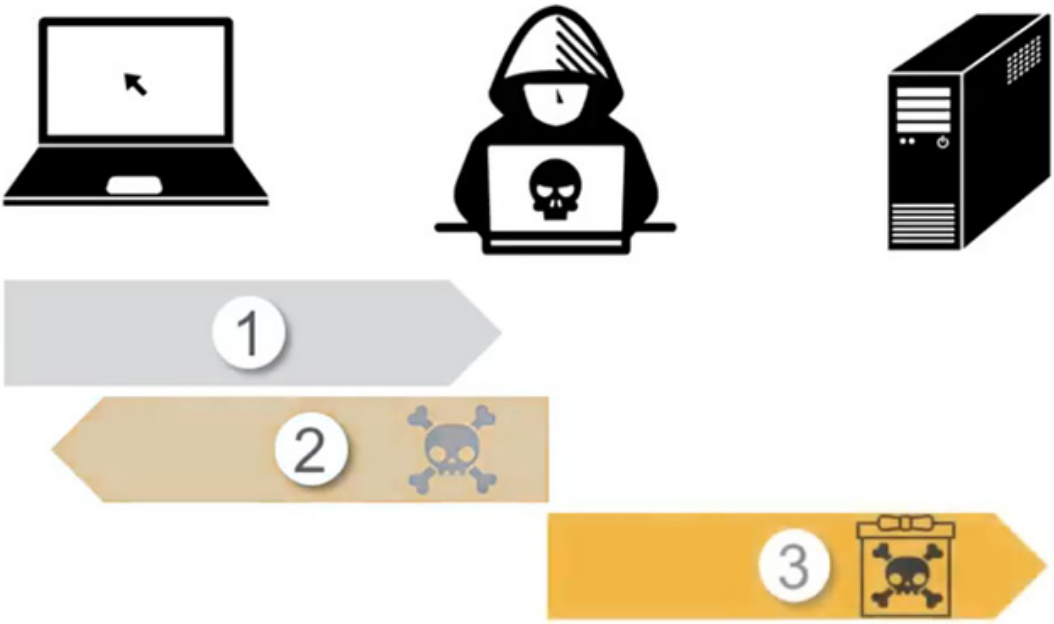
While Intel and Microsoft are still managing its patches for Meltdown and Spectre vulnerabilities, the newly discovered vulnerabilities could create similar trouble for AMD and its customers. It's unclear how long it would take to fix these issues. CTS-Labs said it hasn't heard back from AMD. How long before a fix is available? We don't know. CTS has been in touch with industry experts to try and answer this question. According to experts, firmware vulnerabilities such as MASTERKEY, RYZENFALL and FALLOUT take several months to fix. Hardware vulnerabilities such as CHIMERA cannot be fixed and require a workaround. Producing a workaround may be difficult and cause undesired side-effects.

Read More

Even More

"Official" site

CredSSP Vulnerability Affects RDP and WinRM on All Windows Versions



The March 2018 Patch Tuesday contains a fix for a severe vulnerability affecting the CredSSP protocol; a vulnerability that affects all Windows versions ever released. Security researchers from Preempt say the flaw (CVE-2018-0886) can be abused to run remote commands on gain control over Windows domain controllers, and then expand access to other systems. The research team describes the vulnerability as a "logic" bug in CredSSP.

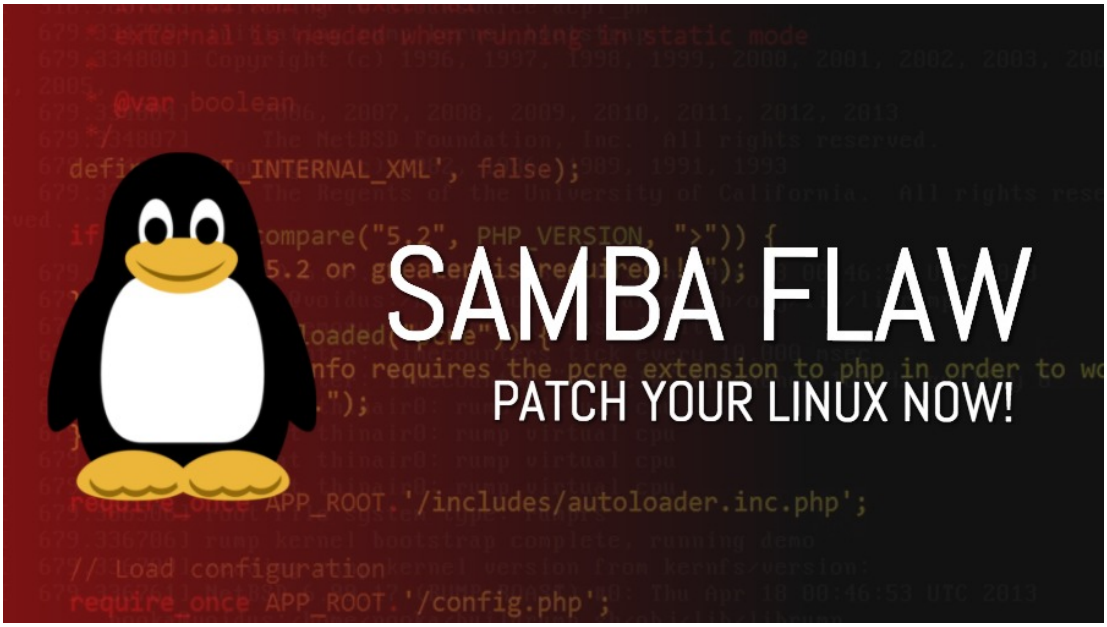
The Credential Security Support Provider (CredSSP) protocol is a Windows-specific mechanism that is responsible for securely forwarding authentication credentials between a client and a remote server in an internal network/domain. CredSSP is a core component of the Remote Desktop Protocol (RDP) and the Windows Remote Management (WinRM) service, both of which are vulnerable to exploitation. An attacker can exploit the CredSSP vulnerability to execute remote commands when users are trying to authenticate during RDP or WinRM sessions.

Because of the nature of this flaw, the attacker needs to have a man-in-the-middle (MitM) position to intercept the victim's traffic. This either means the attacker must have a foothold on an internal network, or control an ISP-level server that relays the victim's RDP session.

Read More

Even More

Samba releases patch to fix two critical vulnerabilities



Samba versions 4.0.0 and up have two critical vulnerabilities that have just been solved by security patches. Samba users should update their instances immediately. The first vulnerability could allow an outside user to launch a DoS attack that takes printing capabilities offline, and the second could allow a remote user to reset user and administrator passwords.

Samba is a free, open source interoperability suite that extends Windows file and print services to Unix and Linux machines. Businesses that run Unix/Linux and Windows side by side frequently use Samba to link the two operating systems together, making any risk to the security and stability of Samba a serious risk. The vulnerabilities in question, CVE-2018-1050 and CVE-2018-1057, are both serious risks for anyone using Samba. If your business has a Samba implementation it's highly recommended that you install the applicable security updates.

As regards the first vulnerability, Samba says there is no known vulnerability associated with the error, only the denial of service resulting from the crash of the spooler. Samba added that leaving the RPC spoolss set to internal prevents the problem from occurring. The second vulnerability, 1057, is a far greater risk to Samba security. This vulnerability only affects Samba installations being used as Active Directory domain controllers, so those using Samba in non-domain control roles don't need to be concerned. If you are using Samba as an AD DC and can't install the security patch yet, there is a workaround Samba says you can put in place as a temporary protection measure: revoking password change permissions for "the world" group.

Read More

Even More

Cutting room floor

- GrayKey iPhone unlocker poses serious security concerns
- Not a breach, Facebook says after suspending firm that took 50M Facebook users' data
- Firefox Master Password System Has Been Poorly Secured for the Past 9 Years
- Chrome Extension Protects Against JavaScript-Based CPU Side-Channel Attacks
- How PayPal Shares Your Data
- How 'Slingshot' Router Malware Lurked for Six Years
- Necurs and Gamut Botnets Account for 97% of the Internet's Spam Emails
- Microsoft Removes Antivirus Registry Key Check for Windows 10 Users
- Report: 77% of companies don't have a consistent cybersecurity response plan
- APT15 Hackers Hit UK Govt Contractor to Steal Military Technology Secrets
- Facebook Flaws Exposed Friend Lists, Payment Card Data
- Let's Encrypt: ACME v2 and Wildcard Certificate Support is Live
- 6 digit PINs and the usefulness of password restrictions
- Flash, Windows Users: It's Time to Patch

#Tech and #Tools

- Top Five Ways I gained access to Your Corporate Wireless Network
- IceBreaker: Gets plaintext Active Directory credentials when on the internal network but outside AD
- Aggressive password policy: When your security turns against you.
- Infection Monkey - An automated pentest tool
- Metta: An information security preparedness tool to do adversarial simulation.
- Top 2Billion passwords
- Analysis of a Kubernetes hack—Backdooring through kubelet
- Bypassing Payments Using Webhooks
- 12 Million Sensitive URLs Available for Download
- Mindmap: Assessment mindset

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