This report is **TLP GREEN**. Recipients may only share **TLP GREEN** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

All information below was shared earlier in today's **TLP WHITE Faith-Based Journal**. This alert provides more detailed explanations and recommendations.

ACTION REQUIRED: "PREVENT A WORM BY UPDATING REMOTE DESKTOP SERVICES." Yesterday, CVE-2019-0708 Remote Desktop Services Remote Code Execution Vulnerability was published. The vulnerability is in the Remote Desktop Services (RDP) component built into some versions of Windows and takes advantage of the RDP service before authentication happens and requires no user interaction (similar to 2017's WannaCry malware outbreak). This vulnerability can lead to complete compromise of a vulnerable system. Pertains to:

- Unsupported Versions of Windows – Windows XP, Windows 2003.
- Supported Versions of Windows – Windows 2008, Windows 7.
- This ***does not*** affect Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012.

Recommendations: Individuals and organizations should conduct patching procedures / execute updates as soon as possible and discuss this threat and response with third-parties / supply chain partners. It is likely that this vulnerability to be weaponized within 24-48 hours. If for some reason you are unable to execute updates, consider network segmentation of unpatched devices and continuous network monitoring of those devices.

In their announcement, Microsoft wrote, that "the vulnerability is 'wormable,' meaning that any future malware that exploits this vulnerability could propagate from vulnerable computer to vulnerable computer in a similar way as the *WannaCry* malware spread across the globe in 2017. While **we have observed no exploitation of this vulnerability**, **it is highly likely that malicious actors will write an exploit for this vulnerability and incorporate it into their malware**." **In other words, *complete updates now*.**

Microsoft continues, "Now that I have your attention, it is important that affected systems are patched as quickly as possible to prevent such a scenario from happening. In response, we are taking the unusual step of providing a security update for all customers to protect Windows platforms, including some out-of-support versions of Windows. Vulnerable in-support systems include Windows 7, Windows Server 2008 R2, and Windows Server 2008. Downloads for in-support versions of Windows can be found in the Microsoft Security Update Guide. Customers who use an in-support version of Windows and have automatic updates enabled are automatically protected. Out-of-support systems include Windows 2003 and Windows XP. If you are on an out-of-support version, the best way to address this vulnerability is to upgrade to the latest version of Windows. Even so, we are making fixes available for these out-of-support versions of Windows in KB4500705."

References:

- **Microsoft**: Prevent a worm by updating Remote Desktop Services (CVE-2019-0708)
- **Krebs on Security**: Microsoft Patches 'Wormable' Flaw in Windows XP, 7 and Windows 2003
- Links to downloads for Windows 7, Windows 2008 R2, and Windows 2008
- Links to downloads for Windows 2003 and Windows XP

ZOMBIELOAD. ZDNet summarizes, "**Academics have discovered a new class of vulnerabilities in Intel processors that can allow attackers to retrieve data being processed inside a CPU**. The leading attack in this new vulnerability class is a security flaw named **Zombieload**, which is another side-channel attack in the same category as Meltdown, Spectre, and Foreshadow… Just like the first three, **Zombieload is exploited by taking advantage of the speculative execution process**,

which is an optimization technique that Intel added to its CPUs to improve data processing speeds and performance. For more than a year, academics have been poking holes in various components of the speculative execution process, revealing ways to leak data from various CPU buffer zones and data processing operations. Meltdown, Spectre, and Foreshadow have shown how various CPU components leak data during the speculative execution process. Today, an international team of academics -- including some of the people involved in the original Meltdown and Spectre research -- along with security researchers from Bitdefender have disclosed a new attack impacting the speculative execution process."

Patches have been released and individuals and organizations should apply these patches as soon as possible. See a number of updates below. For reference: **TechCrunch**: Apple, Amazon, Google, Microsoft and Mozilla release patches for ZombieLoad chip flaws.

See the links above and this link: **ZOMBIELOAD ATTACK** for more details – including common questions and answers - and, of course, a cool logo. Related: How to test MDS (Zombieload) patch status on Windows systems.

Additional Updates include:

- **Apple Releases Multiple Security Updates**. "Apple has released security updates to address vulnerabilities in multiple products. A remote attacker could exploit some of these vulnerabilities to take control of an affected system. The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review the Apple security pages for the following products and apply the necessary updates:
  - watchOS 5.2.1
  - Safari 12.1.1
  - Apple TV Software 7.3
  - tvOS 12.3
  - iOS 12.3
  - macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra

- **Facebook Releases Security Advisory for WhatsApp**. "Facebook has released a security advisory to address a vulnerability in WhatsApp. A remote attacker could exploit this vulnerability to take control of an affected device. The Cybersecurity and Infrastructure Security Agency (CISA) encourages users to review the Facebook Security Advisory for CVE-2019-3568 and upgrade to the appropriate version."

- **Samba Releases Security Updates**. "The Samba Team has released security updates to address a vulnerability in Samba. An attacker could exploit this vulnerability take control of an affected system. The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review the Samba Security Announcement for CVE-2018-16860 and apply the necessary updates."

- **Adobe Releases Security Updates**. "Adobe has released security updates to address vulnerabilities in multiple products. An attacker could exploit some of these vulnerabilities to take control of an affected system. The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review Adobe Security Bulletins APSB19-29, APSB19-26, and APSB19-18 and apply the necessary updates."

- **Microsoft Releases May 2019 Security Updates**. "Microsoft has released updates to address multiple vulnerabilities in Microsoft software. A remote attacker could exploit some of these vulnerabilities to take control of an affected system. The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review Microsoft's May 2019 Security Update Summary and Deployment Information and apply the necessary updates."

Approved for public posting as TLP WHITE by FB-ISAO on 25 June 2019

- **Intel Releases Security Updates, Mitigations for Multiple Products**. “Intel has released security updates and recommendations to address vulnerabilities in multiple products. An attacker could exploit some of these vulnerabilities to take control of an affected system. The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review theIntel Product Security Center Advisories page, apply the necessary mitigations, and refer to vendors for appropriate patches, when available.”

- **VMware Releases Security Updates**. “VMware has released security updates to address vulnerabilities in vCenter Server, ESXi, Workstation, and Fusion. An attacker could exploit some of these vulnerabilities to take control of an affected system. The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review VMware Security Advisories VMSA-2019-0007 and VMSA-2019-0008 and apply the necessary updates.”