AMD admits that its new driver update packages for Windows are becoming a 'shooting target' of hackers

AMD has just published a long list of security flaws and corresponding exploits related to their Windows 10 graphics driver updates.

The company says these vulnerabilities make its driver packages vulnerable to a variety of malicious exploits that can seriously affect the overall security state of the system, including:

1. Escalation of privileges
2. Denial of service
3. Leaking information
4. Skip KASLR
5. Arbitrary writes to kernel memory

The image below shows a list of designated CVE IDs that correspond to the malicious exploit that has been reported by AMD related to its driver update packages, with a brief description and threat level. that they cause.

CVE-2020-12902	High	Arbitrary Decrement Privilege Escalation in AMD Graphics Driver for Windows 10 may lead to escalation of privilege or denial of service.
CVE-2020-12891	High	AMD Radeon Software may be vulnerable to DLL Hijacking through path variable. An unprivileged user may be able to drop its malicious DLL file in any location which is in path environment variable.
CVE-2020-12892	High	An untrusted search path in AMD Radeon settings Installer may lead to a privilege escalation or unauthorized code execution.
CVE-2020-12893	High	Stack Buffer Overflow in AMD Graphics Driver for Windows 10 in Escape 0x15002a may lead to escalation of privilege or denial of service.
CVE-2020-12894	High	Arbitrary Write in AMD Graphics Driver for Windows 10 in Escape 0x40010d may lead to arbitrary write to kernel memory or denial of service.
CVE-2020-12895	High	Pool/Heap Overflow in AMD Graphics Driver for Windows 10 in Escape 0x110037 may lead to escalation of privilege, information disclosure or denial of service.
CVE-2020-12898	High	Stack Buffer Overflow in AMD Graphics Driver for Windows 10 may lead to escalation of privilege or denial of service.
CVE-2020-12901	High	Arbitrary Free After Use in AMD Graphics Driver for Windows 10 may lead to KASLR bypass or information disclosure.
CVE-2020-12903	High	Out of Bounds Write and Read in AMD Graphics Driver for Windows 10 in Escape 0x6002d03 may lead to escalation of privilege or denial of service.
CVE-2020-12900	High	An arbitrary write vulnerability in the AMD Radeon Graphics Driver for Windows 10 potentially allows unprivileged users to gain Escalation of Privileges and cause Denial of Service.
CVE-2020-12929	High	Improper parameters validation in some trusted applications of the PSP contained in the AMD Graphics Driver may allow a local attacker to bypass security restrictions and achieve arbitrary code execution.
CVE-2020-12960	High	AMD Graphics Driver for Windows 10, amdfender.sys may improperly handle input validation on InputBuffer which may result in a denial of service (DoS).
CVE-2020-12980	High	An out of bounds write and read vulnerability in the AMD Graphics Driver for Windows 10 may lead to escalation of privilege or denial of service.
CVE-2020-12981	High	An insufficient input validation in the AMD Graphics Driver for Windows 10 may allow unprivileged users to unload the driver, potentially causing memory corruptions in high privileged processes, which can lead to escalation of privileges or denial of service.
CVE-2020-12982	High	An invalid object pointer free vulnerability in the AMD Graphics Driver for Windows 10 may lead to escalation of privilege or denial of service.
CVE-2020-12983	High	An out of bounds write vulnerability in the AMD Graphics Driver for Windows 10 may lead to escalation of privileges or denial of service.
CVE-2020-12985	High	An insufficient pointer validation vulnerability in the AMD Graphics Driver for Windows 10 may lead to escalation of privilege or denial of service.
CVE-2020-12986	High	An insufficient pointer validation vulnerability in the AMD Graphics Driver for Windows 10 may cause arbitrary code execution in the kernel, leading to escalation of privilege or denial of service.
CVE-2020-12962	Medium	Escape call interface in the AMD Graphics Driver for Windows may cause privilege escalation.
CVE-2020-12904	Medium	Out of Bounds Read in AMD Graphics Driver for Windows 10 in Escape 0x3004203 may lead to arbitrary information disclosure.
CVE-2020-12905	Medium	Out of Bounds Read in AMD Graphics Driver for Windows 10 in Escape 0x3004403 may lead to arbitrary information disclosure.
CVE-2020-12964	Medium	A potential privilege escalation/denial of service issue exists in the AMD Radeon Kernel Mode driver Escape 0x2000c00 Call handler. An attacker with low privilege could potentially induce a Windows BugCheck or write to leak information.
CVE-2020-12987	Medium	A heap information leak/kernel pool address disclosure vulnerability in the AMD Graphics Driver for Windows 10 may lead to KASLR bypass.
CVE-2020-12920	Medium	A potential denial of service issue exists in the AMD Display driver Escape 0x130007 Call handler. An attacker with low privilege could potentially induce a Windows BugCheck
CVE-2020-12899	Medium	Arbitrary Read in AMD Graphics Driver for Windows 10 may lead to KASLR bypass or denial of service.
CVE-2020-12897	Medium	Kernel Pool Address disclosure in AMD Graphics Driver for Windows 10 may lead to KASLR bypass.
CVE-2020-12963	Medium	An insufficient pointer validation vulnerability in the AMD Graphics Driver for Windows may allow unprivileged users to compromise the system.

In fact, the majority of the above-mentioned vulnerabilities were discovered and reported by third-party security researchers. In which, Ori Nimron (Twitter username @orinimron123) is the white hat hacker with the largest contribution. AMD said that the company has been gradually rolling out patches for known vulnerabilities through additional graphics driver updates. The most recent update with code 21.4.1, also a major 2020-21 driver update for Radeon graphics cards, not only comes with patches, but also brings a lot of new features as well as improvements. improve the stability in the operation of the hardware.

It is quite a coincidence that Intel is also struggling with the same situation. That's because Intel built its Kaby Lake G SKUs using AMD's Vega graphics. Therefore, 'Team Blue' also had to rush to release new graphics

driver version 21.10.03.11 for the Kaby Lake G series to fix the problem, despite the product line being discontinued (EOL) quite a while ago.

In addition to the bugs noted by AMD, Intel also added one more bug discovered and tracked by themselves with the identifier "CVE-2021-33105". More information can be found on Intel's website.