Clarification About the Recent Vulnerabilities

We would like to address the many technical points and misunderstandings with a few technical clarifications about the vulnerabilities.

The vulnerabilities described in our site are second-stage vulnerabilities. What this means is that the vulnerabilities are mostly relevant for enterprise networks, organizations and cloud providers.

Computers on enterprise networks occasionally get compromised - whether through phishing attempts, zero-day exploits or employees downloading the wrong file. High-security enterprise networks are equipped to deal with these kinds of "every-day" attacks. They do this by keeping their systems up to date, enabling security features, and employing additional measures such as endpoint security solutions.

The vulnerabilities described in *amdflaws.com* could give an attacker that has already gained initial foothold into one or more computers in the enterprise a significant advantage against IT and security teams.

The only thing the attacker would need after the initial local compromise is local admin privileges and an affected machine. To clarify misunderstandings – there is no need for physical access, no digital signatures, no additional vulnerability to reflash an unsigned BIOS. Buy a computer from the store, run the exploits as admin – and they will work (on the affected models as described on the site).

Attackers in possession of these vulnerabilities would receive the following additional capabilities:

- **Persistency**: Attackers could load malware into the AMD Secure Processor before the CPU starts. From this position they can prevent further BIOS updates and remain hidden from security products. This level of persistency is extreme – even if you reinstall the OS or try to reflash the BIOS – a sophisticated attacker can survive it. The only way to remove the attacker from the chip, as far as we know would be to start soldering out chips or to connect an external programmer to the SPI chip. (we have seen a motherboard that had a socket where you can switch chips – then you could just put a new SPI chip).

- **Stealth**: Sitting inside the AMD Secure Processor or the AMD Chipset or the System Management Mode (SMM) is, at the moment, outside the reach of virtually all security products. AMD chips could become a safe haven for attackers to operate from.

- **Network Credential Theft**: The ability to bypass Microsoft Credentials Guard and steal network credentials, for example credentials left by the IT department on the affected machine. We have a PoC version of mimikatz that works even with Credential Guard enabled. Stealing domain credentials could help attackers to move to higher value targets in the network.

- Specific AMD Secure Processor features for cloud providers, such as Secure Encrypted Virtualization (SEV) could be circumvented or disabled by these vulnerabilities.

What was it tested on?

These are the machines we have tested the vulnerabilities on. On our site, every red circle in the vulnerabilities map represents a working PoC that was tested in our lab.

This is the list of hardware that has been tested in our lab:

- BIOSTAR B350 GT3 Ryzen Motherboard.
- GIGABYTE AB350-GAMING 3
- HP EliteDesk 705 G3 SFF Ryzen Pro machine
- HP Envy X360 Ryzen Mobile Laptop
- TYAN B8026T70AV16E8HR EPYC SERVER
- GIGABYTE MZ31-AR0 EPYC SERVER

RYZENFALL, FALLOUT

Requirements

- Physical access is not required. An attacker would only need to be able to run an EXE with local admin privileges on the machine.

Impact:

- Write to SMM memory, leading to code execution in SMM.
- Reading and/or tampering with Credential Guard VTL-1 memory through the PSP.
- Ryzenfall-4, which achieves code execution inside the PSP, leads to all the attacker capabilities described above, as well as the capability to tamper with the PSP and its security features.
- An attacker can use RYZENFALL or FALLOUT to bypass Windows Credential Guard, steal network credentials, and then use these to move laterally through Windows-based enterprise networks.

MASTERKEY

Requirements:

- Physical access is not required. An attacker would only need to be able to run an EXE with local admin privileges on the machine.
- Wait for reboot.

Impact:

The MASTERKEY set of vulnerabilities enable an attacker to execute unsigned code inside the PSP. Totaling a complete compromise of the Secure Processor. The exploit reflashes the BIOS to take advantage of the vulnerability:

- On some motherboards – this works out of the box. This is because PSP firmware is often ignored by BIOS signature checks.
- In other cases – RYZENFALL #1-2 or FALLOUT #1-#2 could be used as a prerequisite for MASTERKEY to achieve code execution in SMM and bypass BIOS signature checks made in SMM code.
- Even if all else fails, we believe using RYZENFALL-4 to write to SPI flash from inside the PSP is probably possible.

CHIMERA

Requirements:

- Physical access is not required. An attacker would only need to be able to run an EXE with local admin privileges on the machine.

Impact:

The CHIMERA set of vulnerabilities are a set Manufacturer Backdoors left on the AMD Chipset, developed by Taiwanese company ASMedia.

- This allows for an attacker to inject malicious code into the chip and take over the chipset (Read/Write/Execute).
- One set of backdoors in implemented in firmware, while the other is implemented in the actual logic gates of the chip (ASIC). Both yield to the same impact.