Severe Security Advisory on AMD Processors

Foreword

This document is meant to inform about multiple critical security vulnerabilities and exploitable manufacturer backdoors inside AMD's latest EPYC, Ryzen, Ryzen Pro, and Ryzen Mobile lines of processors. These vulnerabilities have the potential to put organizations at significantly increased risk of cyber-attacks.

To ensure public safety, all technical details that could be used to reproduce the vulnerabilities have been redacted from this document. CTS has privately shared this information with AMD, select security companies that can develop mitigations, and the U.S. regulators. What follows is a description of the security problems we discovered and the risks they pose for users and organizations.[1]

Critical Security Vulnerabilities in AMD Processors

Over the past year AMD has introduced an array of new technologies targeting critical applications in the enterprise, industrial, and aerospace sectors. As the company expands from the consumer market into these new areas, security is fast becoming a key component of its offering.

CTS has been researching the security of AMD's latest *Zen* processors for the past six months, including *EPYC*, *Ryzen*, *Ryzen Pro* and *Ryzen Mobile*, and has made concerning discoveries:

1. The *AMD Secure Processor*, the gatekeeper responsible for the security of AMD processors, contains critical vulnerabilities. This integral part of most of AMD's products, including workstations and servers, is currently being shipped with multiple security vulnerabilities that could allow malicious actors ("attackers") *to permanently install malicious code inside the Secure Processor itself*. These vulnerabilities could expose AMD customers to industrial espionage that is virtually undetectable by most security solutions.

2. A set of security vulnerabilities in the *Secure Processor* could allow attackers to steal network credentials – even on systems guarded by Microsoft's latest *Credential Guard* technology. This could allow attackers to spread through otherwise secure and up-to-date corporate networks.

3. *Secure Encrypted Virtualization*, a key security feature that AMD advertises as one of its main offerings to cloud providers – could be defeated as soon as attackers obtain malicious code execution on the *EPYC Secure Processor*.

4. The *Ryzen* chipset, a core system component that AMD outsourced to a Taiwanese chip manufacturer, ASMedia, is currently being shipped with exploitable manufacturer backdoors inside. These backdoors could allow attackers to inject malicious code into the chip. The chipset is a central component on the motherboard, responsible for linking the *Ryzen* processor with hardware devices

[1] See additional legal disclosure at the end of this paper.

such as WiFi and network cards, making it an ideal target for attackers.

We note with concern that AMD’s outsource partner, ASMedia, is a subsidiary of ASUSTeK Computer, a company that has recently been penalized by the Federal Trade Commission for neglecting security vulnerabilities and put under mandatory external security audits for the next 20 years.[2]

CTS believes that networks that contain AMD computers are at a considerable risk. The vulnerabilities we have discovered allow bad actors who infiltrated the network to persist in it, surviving computer reboots and reinstallations of the operating system, while remaining virtually undetectable by most endpoint security solutions. This allows attackers to engage in persistent, virtually undetectable espionage, buried deep in the system and executed from AMD’s *Secure Processor* and chipset.

In our opinion, the basic nature of some of these vulnerabilities amounts to complete disregard of fundamental security principles. This raises concerning questions regarding security practices, auditing, and quality controls at AMD.

[2] https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

Concerns Regarding Insufficient Security Quality Controls

Many of the vulnerabilities described in this document are indications of poor security practices and insufficient security quality controls. The *Ryzen* and *Ryzen Pro* chipsets, currently shipping with exploitable backdoors, could not have passed even the most rudimentary white-box security review. The *Secure Processor*, currently shipping with no fewer than *ten* critical vulnerabilities that bypass most of its security features, is afflicted with basic security design errors[3]. Furthermore, neither the Security Processor nor the Chipset offer any significant mitigations against exploitation should a vulnerability be discovered.

In the meantime, the *Zen architecture* is a tremendous success. *EPYC* servers are in the process of being integrated into datacenters around the world, including at Baidu and Microsoft Azure Cloud[4], and AMD has recently announced that *EPYC* and *Ryzen* embedded processors are being sold as high-security solutions for mission-critical aerospace and defense systems[5]. AMD's latest generation Vega GPUs, which also have *Secure Processor* inside of them, are being integrated as deep-learning accelerators on self-driving cars[6].

Source: https://www.facebook.com/AMD/videos/10156221257721473/

We urge the security community to study the security of these devices in depth before allowing them on mission-critical systems that could potentially put lives at risk.

[3] For example, the *MASTERKEY-2* vulnerability could be attributed to a basic design flaw in the *Cryptographic Coprocessor*.

[4] https://www.forbes.com/sites/moorinsights/2017/12/14/amd-wins-another-cloud-provider-with-baidu-abc-services/

[5] https://www.amd.com/Documents/Aerospace-and-Defense-Application-Brief.pdf

[6] https://www.forbes.com/sites/kenkam/2017/11/29/nvidias-advantage-in-self-driving-cars-will-be-hard-for-intel-and-amd-to-overcome/

Table of Contents

Foreword....1

Critical Security Vulnerabilities in AMD Processors....1

Concerns Regarding Insufficient Security Quality Controls....3

Vulnerabilities....5

Overview....5

Background on AMD Secure Processor....7

MASTERKEY: Unauthorized Code Execution and Malware Persistency on AMD Secure Processor....8

Background....8

The MASTERKEY Vulnerabilities....8

Affected Processors....10

Mitigations....10

RYZENFALL: Vulnerabilities in Ryzen Secure Processor....11

Impacts and Prerequisites for Exploitation....12

Mitigations....13

Affected Processors....13

FALLOUT: Vulnerabilities in EPYC Server Secure Processor....14

Impacts and Prerequisites for Exploitation....14

Mitigations....15

Affected Processors....15

CHIMERA: Backdoors Inside Ryzen Chipset....16

Third-Party Chip Design Plagued with Hidden Backdoors....17

Prerequisites for Exploitation....18

Affected Processors....18

Mitigations....18

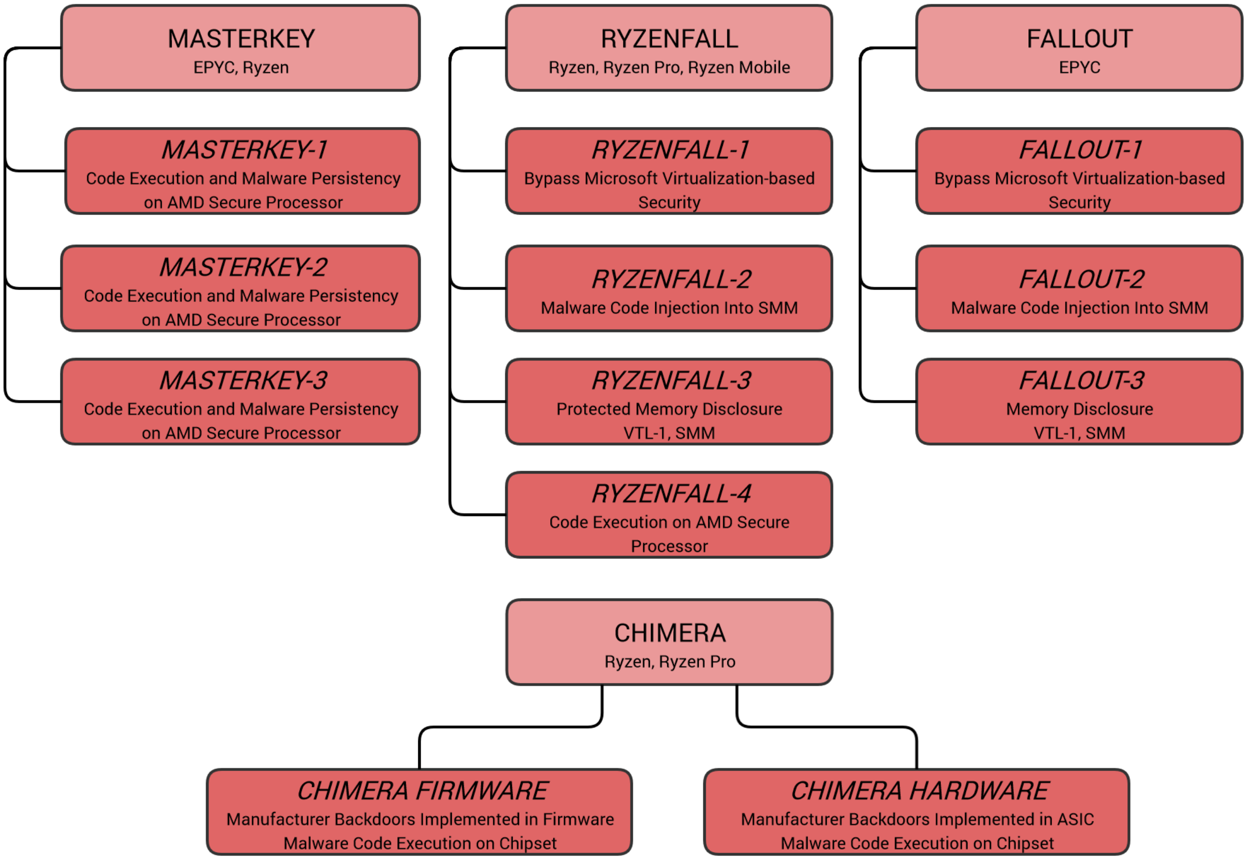
Conclusion....19

Important Legal Disclaimer....20

Vulnerabilities

Overview

This document describes four classes of vulnerabilities present on AMD *Zen architecture* processors and chipsets. Each class contains within it several different vulnerabilities. A summary of these vulnerabilities and the affected hardware is provided below:



MASTERKEY
EPYC, Ryzen

MASTERKEY-1
Code Execution and Malware Persistency on AMD Secure Processor

MASTERKEY-2
Code Execution and Malware Persistency on AMD Secure Processor

MASTERKEY-3
Code Execution and Malware Persistency on AMD Secure Processor

RYZENFALL
Ryzen, Ryzen Pro, Ryzen Mobile

RYZENFALL-1
Bypass Microsoft Virtualization-based Security

RYZENFALL-2
Malware Code Injection Into SMM

RYZENFALL-3
Protected Memory Disclosure
VTL-1, SMM

RYZENFALL-4
Code Execution on AMD Secure Processor

FALLOUT
EPYC

FALLOUT-1
Bypass Microsoft Virtualization-based Security

FALLOUT-2
Malware Code Injection Into SMM

FALLOUT-3
Memory Disclosure
VTL-1, SMM

CHIMERA
Ryzen, Ryzen Pro

CHIMERA FIRMWARE
Manufacturer Backdoors Implemented in Firmware
Malware Code Execution on Chipset

CHIMERA HARDWARE
Manufacturer Backdoors Implemented in ASIC
Malware Code Execution on Chipset

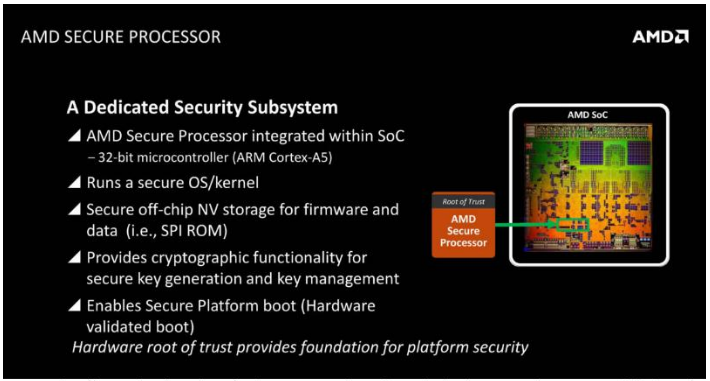
Vulnerabilities	Impact
MASTERKEY-1 ***MASTERKEY-2*** ***MASTERKEY-3***	▪ Persistent malware running inside AMD Secure Processor ▪ Bypass firmware-based security features such as *Secure Encrypted Virtualization* (SEV) and *Firmware Trusted Platform Module* (fTPM) ▪ Network credential theft. Bypass *Microsoft Virtualization-based Security* (VBS), including *Windows Credential Guard* ▪ Physical damage to hardware (SPI flash wear-out, etc.) ▪ Affects: *EPYC, Ryzen, Ryzen Pro, Ryzen Mobile*. Successfully exploited on *EPYC* and *Ryzen*

RYZENFALL-1 ***FALLOUT-1***	▪ Write to protected memory areas, including: o Windows Isolated User Mode and Isolated Kernel Mode (VTL1) o AMD Secure Processor Fenced DRAM – Allows direct tampering with trusted code running on AMD Secure Processor. Only applicable to select *Ryzen* motherboards ▪ Network credential theft. Bypass *Microsoft Virtualization-based Security (VBS)* including *Windows Credential Guard* ▪ Enables memory-resident *VTL1* malware that is resilient against most endpoint security solutions ▪ Affects: *EPYC, Ryzen, Ryzen Pro, Ryzen Mobile*. Successfully exploited on *EPYC*, *Ryzen*, *Ryzen Pro* and *Ryzen Mobile*
RYZENFALL-2 ***FALLOUT-2***	▪ Disable *Secure Management RAM (SMRAM)* read/write protection ▪ Enables memory-resident SMM malware, resilient against most endpoint security solutions ▪ Affects: *EPYC, Ryzen, Ryzen Pro.* Successfully exploited on *EPYC, Ryzen, Ryzen Pro*. *Ryzen Mobile* is not affected
RYZENFALL-3 ***FALLOUT-3***	▪ Read from protected memory areas, including: o Windows Isolated User Mode and Isolated Kernel Mode (VTL1) o Secure Management RAM (SMRAM) o AMD Secure Processor Fenced DRAM. Only applicable to select *Ryzen* motherboards ▪ Network credential theft. Bypass *Windows Credential Guard* by reading secrets from VTL1 memory ▪ Affects: *EPYC, Ryzen, Ryzen Pro.* Successfully exploited on *EPYC, Ryzen, Ryzen Pro*. *Ryzen Mobile* is not affected
RYZENFALL-4	▪ Arbitrary code execution on AMD Secure Processor ▪ Bypass firmware-based security features such as *Firmware Trusted Platform Module* (fTPM) ▪ Network credential theft. Bypass *Microsoft Virtualization-based Security* (VBS), including *Windows Credential Guard* ▪ Physical damage to hardware (SPI flash wear-out, etc.) ▪ Affects: *Ryzen, Ryzen Pro.* Successfully exploited on *Ryzen, Ryzen Pro*.
CHIMERA-FW ***CHIMERA-HW***	▪ Two sets of manufacturer backdoors: One implemented in firmware, the other in hardware (ASIC) ▪ Allows malware to inject itself into the chipset's internal *8051 architecture* processor ▪ The chipset links the CPU to USB, SATA, and PCI-E devices. Network, WiFi and Bluetooth traffic often flows through the chipset as well ▪ Malware running inside the chipset could take advantage of the chipset's unique position as a middleman for hardware peripherals ▪ Affects: *Ryzen, Ryzen Pro*. Successfully exploited on *Ryzen* and *Ryzen Pro*.

Background on AMD Secure Processor

The *AMD Secure Processor* is a security subsystem introduced by AMD in 2013. On the new *Zen architecture*, *Secure Processor* has been thoroughly revised to incorporate advanced features such as *Secure Memory Encryption (SME)*, *Secure Encrypted Virtualization (SEV)* and *Firmware Trusted Platform Module (fTPM)*.

The *Secure Processor* is a 32-bit ARM Cortex A5 processor that sits alongside the main CPU inside the chip. It is responsible for creating, monitoring and maintaining the security environment. Its functions include managing the boot process, initializing various security related mechanisms, and monitoring the system for any suspicious activity or events, and implementing an appropriate response[7].



AMD SECURE PROCESSOR

AMD

A Dedicated Security Subsystem

- AMD Secure Processor integrated within SoC
  – 32-bit microcontroller (ARM Cortex-A5)
- Runs a secure OS/kernel
- Secure off-chip NV storage for firmware and data (i.e., SPI ROM)
- Provides cryptographic functionality for secure key generation and key management
- Enables Secure Platform boot (Hardware validated boot)

Hardware root of trust provides foundation for platform security

Source: http://www.redgamingtech.com/amd-zen-processors-feature-impressive-hardware-encryption-not-present-in-intel-cpus/

One of the primary functions of the *Secure Processor* is to act as the immutable *Root of Trust* for verifying the secure boot process. This feature allows for AMD's *Hardware Validated Boot*.

The *Secure Processor* is ubiquitous and can be found on virtually all of AMD's newer products, including *Ryzen* and *EPYC* processors, *Vega* GPUs, APUs, and mobile and embedded processors.

Since its early days the *AMD Secure Processor* has been a center of controversy within the open-source and security communities. Critics are concerned that the *Secure Processor* is a black box: few understand how it actually works, yet it has complete access to the system, and its actions are highly privileged and mostly invisible to the operating system. There have been petitions asking AMD to open-source the *Secure Processor*, but AMD refused.[8] The company emphasized that it has performed extensive security audits on the *Secure Processor*, and that it is secure.[9]

[7] https://en.wikipedia.org/wiki/AMD_Platform_Security_Processor
[8] https://libreboot.org/amd-libre.html
[9] https://www.pscp.tv/AMDServer/1eaKbmEwypQxX

MASTERKEY: Unauthorized Code Execution and Malware Persistency on AMD Secure Processor

Background

AMD Hardware Validated Boot

Hardware Validated Boot (HVB) is an AMD-specific form of *Secure Boot* that roots the trust to hardware in an immutable *Read-only Memory (ROM)*, which runs inside a dedicated *Secure* Processor. The *Secure Processor* then verifies the integrity of the system ROM firmware (BIOS).

The *Secure Processor* ROM contains the initial immutable code, also known as the *Root of Trust*. The ROM validates a secure boot key and then uses the key to validate the larger *Secure Processor* firmware, which it reads from system flash. The *Secure Processor* then validates the BIOS platform-initialization code before allowing it to run. AMD calls this feature *Hardware Validated Boot.*[10]

UEFI Secure Boot

UEFI Secure Boot is a security standard developed by members of the PC industry to help make sure that a device boots using only software that is trusted by the Original Equipment Manufacturer (OEM). When the PC starts, the BIOS firmware checks the signature of each piece of boot software, including UEFI firmware drivers (also known as Option ROMs), EFI applications, and the operating system. If the signatures are valid, the PC boots, and the firmware gives control to the operating system.[11]

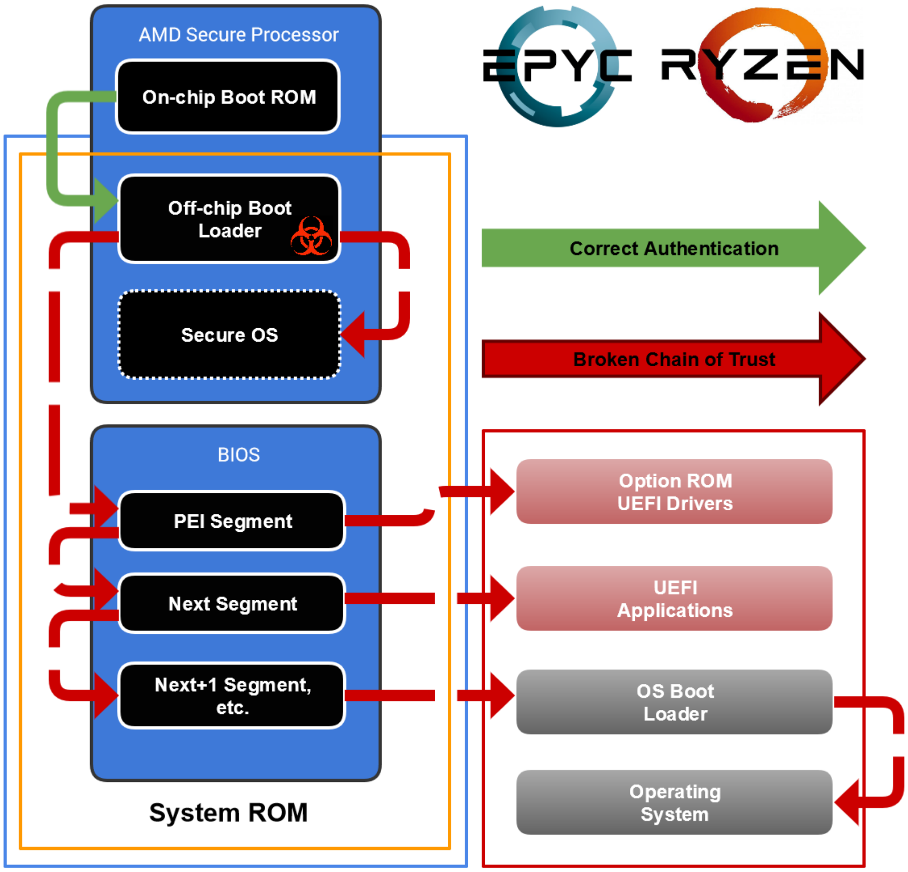
The process of *Secure Boot* is critical for maintaining security. It mitigates against severe threat scenarios such as: (a) Malware that loads at the early stages of boot, allowing it to disable any security solution that loads after it, and (b) Supply chain attacks: hardware peripherals with malware-carrying Option ROMs that inject code into the BIOS.

The MASTERKEY Vulnerabilities

MASTERKEY is a set of three vulnerabilities allowing three distinct pathways to bypass *Hardware Validated Boot* on *EPYC* and *Ryzen* and achieve arbitrary code execution on the *Secure Processor* itself. The vulnerabilities allow malicious actors to install persistent malware inside the *Secure Processor*, running in kernel-mode with the highest possible permissions. From this position of power, a malware is able to bypass *Secure Boot* and inject malicious code into the BIOS or operating system, as well as to disable any firmware-based security features within the *Secure Processor* itself, such as *Firmware Trusted Platform Module (fTPM)* or *Secure Encrypted Virtualization (SEV)*.

[10] https://ebrary.net/24869/computer_science/secure_technology

[11] https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot



MASTERKEY Vulnerabilities

Multiple Bypasses for Hardware Validated Boot

Exploiting *MASTERKEY* requires an attacker to be able to re-flash the BIOS with a specially crafted BIOS update. This update would contain *Secure Processor* metadata that exploits one of the vulnerabilities, as well as malware code compiled for *ARM Cortex A5* – the processor inside the *AMD Secure Processor*. Because the *Secure Processor* checks its own digital signatures, this malicious update often passes BIOS-specific digital signature verifications.

MASTERKEY can often be exploited as part of a remote cyber-attack. Most *EPYC* and *Ryzen* motherboards on the market use a BIOS by American Megatrends that allows easy re-flashing from within the operating system using a command-line utility. Such utility could be used by remote attackers in the course of a cyber-attack.

On motherboards where re-flashing is not possible because it has been blocked, or because BIOS updates must be encapsulated and digitally signed by an OEM-specific digital signature, we suspect an attacker could occasionally still succeed in re-flashing the BIOS. This could be done by first exploiting *RYZENFALL* or *FALLOUT* and breaking into *System Management Mode (SMM)*. SMM privileges could then be used to write to system flash, assuming the latter has not been permanently write-locked.

Affected Processors

CTS has successfully exploited *MASTERKEY-1* and *MASTERKEY-2* on *EPYC* and *Ryzen*. We did not attempt to produce exploits for *Ryzen Pro* and *Ryzen Mobile*, although we have seen the vulnerabilities in the code. We also did not attempt to produce exploits for *MASTERKEY-3*.

Vulnerability	Affected Processors	Impact
MASTERKEY-1	*EPYC Server* *Ryzen* *Ryzen Pro* *Ryzen Mobile*	▪ Install persistent malware inside *AMD Secure Processor* ▪ Disable security features such as *Firmware Trusted Platform Module* or *Secure Encrypted Virtualization*.
MASTERKEY-2	*EPYC Server* *Ryzen* *Ryzen Pro* *Ryzen Mobile*	▪ Install persistent malware inside *AMD Secure Processor* ▪ Disable security features such as *Firmware Trusted Platform Module* or *Secure Encrypted Virtualization*.
MASTERKEY-3	*EPYC Server* *Ryzen* *Ryzen Pro* *Ryzen Mobile*	▪ Install persistent malware inside *AMD Secure Processor* ▪ Disable security features such as *Firmware Trusted Platform Module* or *Secure Encrypted Virtualization*.

Visual demonstration of unauthorized code execution on EPYC Secure Processor
Hardware: TYAN B8026 (Single Socket EPYC Server)

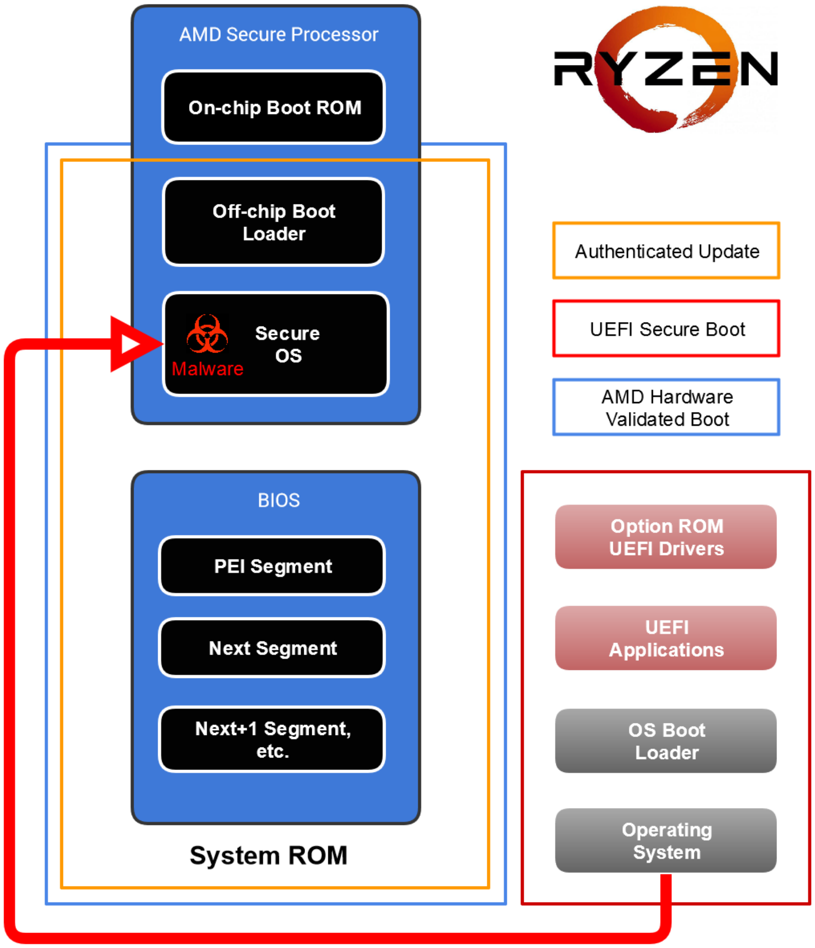
Mitigations

- Consult with your OEM on ways to prevent unauthorized BIOS updates
- Machines that are also vulnerable to *RYZENFALL* are at increased risk of attack, because a compromised *Secure Processor* may be able to circumvent OEM-specific mitigations and write to system flash.

RYZENFALL: Vulnerabilities in Ryzen Secure Processor

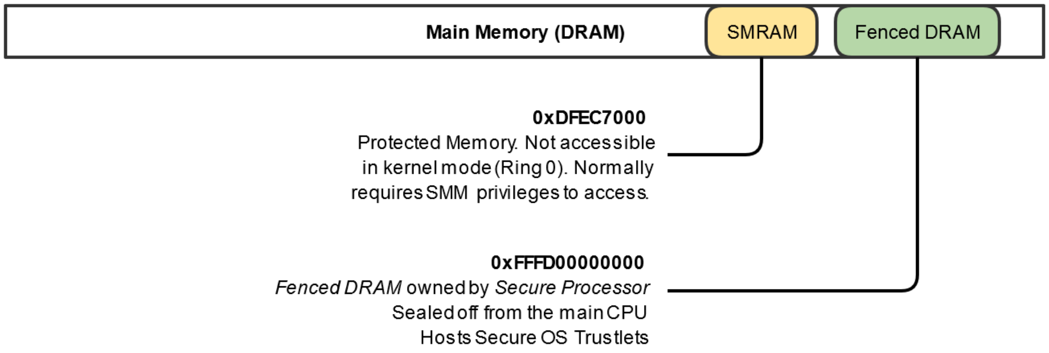
The RYZENFALL vulnerabilities are a set of design and implementation flaws inside *AMD Secure OS* – the operating system powering *AMD Secure Processor* on *Ryzen, Ryzen Pro* and *Ryzen Mobile*. The vulnerabilities allow, at their worst, for the *Secure Processor* to be completely taken over by malware running on the main processor.

Secure OS is only found on *Ryzen, Ryzen Pro* and *Ryzen Mobile.* It is based on *T-Base* by *Trustonic*, and leverages *ARM Trust Zone®* technology for secure isolation between system components. One of the primary features implemented on top of *Secure OS* is AMD's *Firmware Trusted Platform Module (fTPM)*, which is responsible for secure storage of passwords and cryptographic secrets.



RYZENFALL Attack

Although *Secure OS* runs inside the *Secure Processor*'s dedicated *ARM Cortex A5* processor, it does make use of the computer's main memory. When *Secure OS* starts, it allocates a portion of main memory for its own use and seals it off from the main processor. This area is called *Fenced DRAM*.


Main Memory (DRAM)
SMRAM
Fenced DRAM
0xDFEC7000
Protected Memory. Not accessible in kernel mode (Ring 0). Normally requires SMM privileges to access.
0xFFFD00000000
Fenced DRAM owned by *Secure Processor*
Sealed off from the main CPU
Hosts Secure OS Trustlets

Impacts and Prerequisites for Exploitation

Exploitation requires that an attacker be able to run a program with local-machine elevated administrator privileges. Accessing the *Secure Processor* is done through a vendor supplied driver that is digitally signed.

The RYZENFALL vulnerabilities allow unauthorized code execution on the *Secure Processor*. They also allow access to protected memory regions that are otherwise sealed off by hardware. Such areas are supposed to be completely inaccessible to both kernel drivers and programs running inside the operating system. These regions are:

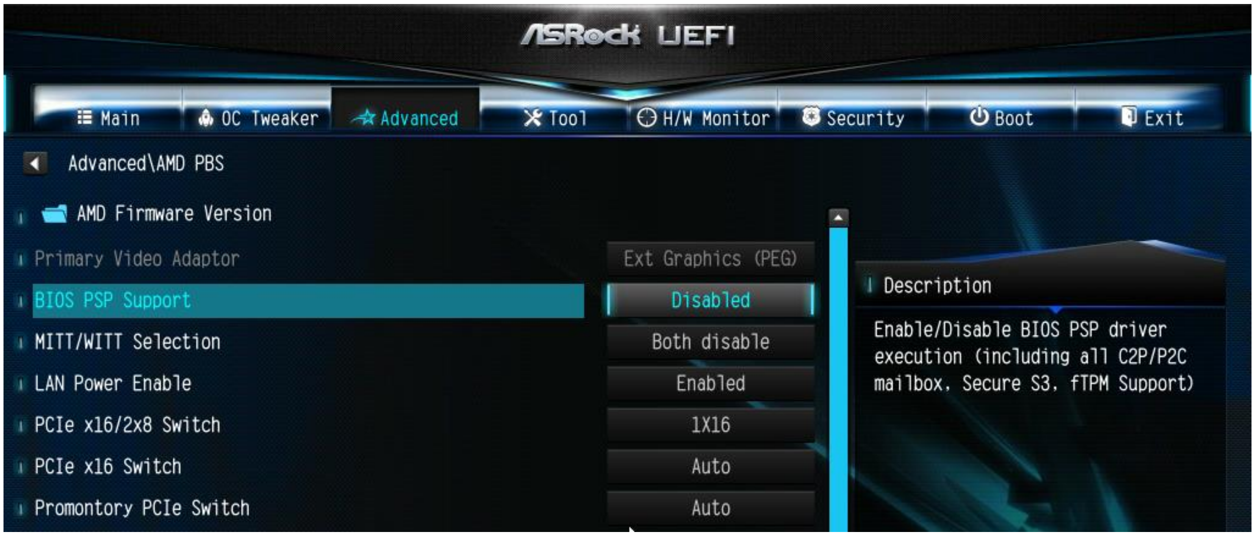
- Windows Isolated User Mode and Isolated Kernel Mode (VTL1)
- Secure Management RAM (SMRAM)
- AMD Secure Processor Fenced DRAM

Breaking this hardware security seal could have severe implications on security. To give some examples, it could allow attackers to:

- Bypass *Microsoft Virtualization-based Security* and steal network credentials. Credential theft is often a precursor to lateral movement inside networks as part of a remote cyber-attack.
- Inject malware into SMM, placing malware outside the reach of endpoint security solutions running on the operating system or even on the hypervisor.
- Disable protections against unauthorized BIOS re-flashing that are implemented in SMM.
- Inject malware into VTL1, placing malware outside the reach of most endpoint security solutions running on the operating system.
- Inject malware into the *AMD Secure Processor* itself.
- If code execution on the *AMD Secure Processor* is achieved – Bypass or tamper firmware-based security features such as *fTPM*.

Mitigations

No known mitigations. AMD has recently released a BIOS update that supposedly allows users disable the *Secure Processor*, but this feature works only partially and does not stop the *RYZENFALL* attacks.



Advanced\AMD PBS

AMD Firmware Version

Primary Video Adaptor	Ext Graphics (PEG)
BIOS PSP Support	Disabled
MITT/WITT Selection	Both disable
LAN Power Enable	Enabled
PCIe x16/2x8 Switch	1X16
PCIe x16 Switch	Auto
Promontory PCIe Switch	Auto

Description

Enable/Disable BIOS PSP driver execution (including all C2P/P2C mailbox, Secure S3, fTPM Support)

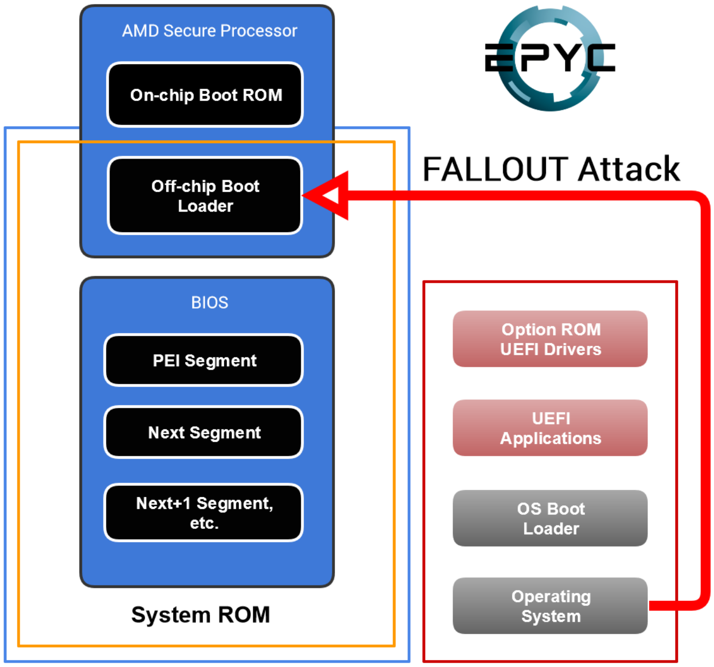
Disable PSP support has no effect on RYZENFALL

Affected Processors

Vulnerability	Affected Processors	Impact
RYZENFALL-1	*Ryzen* *Ryzen Pro* *Ryzen Mobile*	*VTL-1* memory write
RYZENFALL-2	*Ryzen* *Ryzen Pro*	Disable SMM protection
RYZENFALL-3	*Ryzen* *Ryzen Pro*	*VTL-1* memory read *SMM* memory read (requires *RYZENFALL-2*)
RYZENFALL-4	*Ryzen* *Ryzen Pro*	Arbitrary code execution on *Secure Processor*

FALLOUT: Vulnerabilities in EPYC Server Secure Processor

The FALLOUT vulnerabilities are a set of design-flaw vulnerabilities residing inside the boot loader component of *EPYC*'s *Secure Processor*. The boot loader is responsible for *Hardware Validated Boot* on *EPYC* servers, as well as for launching the *Secure Processor* module for *Secure Encrypted Virtualization (SEV)*.



Impacts and Prerequisites for Exploitation

Exploitation requires that an attacker be able to run a program with local-machine elevated administrator privileges. Accessing the *Secure Processor* is done through a vendor supplied driver that is digitally signed.

The FALLOUT vulnerabilities allows access to protected memory regions that are otherwise sealed off by hardware. Such areas are supposed to be completely inaccessible to both kernel drivers and user programs running inside the operating system. These regions are:

- Windows Isolated User Mode and Isolated Kernel Mode (VTL1)
- Secure Management RAM (SMRAM)

Breaking this hardware security seal could have severe implications on security. To give some examples, it could allow attackers to:

- Bypass *Microsoft Virtualization-based Security* and steal network credentials. Credential theft is often a precursor to lateral movement inside networks as part of a remote cyber-attack.
- Inject malware into SMM, placing malware outside the reach of endpoint security solutions running on the operating system or even on the hypervisor.
- Disable protections against unauthorized BIOS re-flashing that are implemented in SMM.
- Inject malware into VTL1, placing malware outside the reach of most endpoint security solutions running on the operating system.

Mitigations

No known mitigations.

Affected Processors

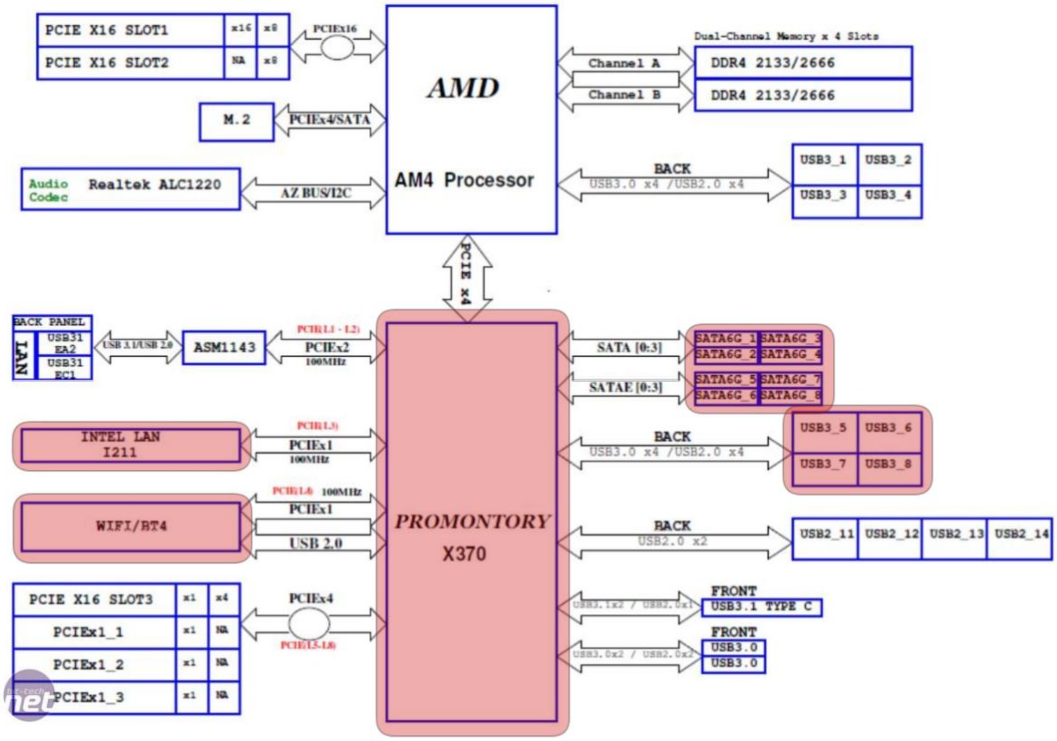
Vulnerability	Affected Processors	Impact
FALLOUT-1	*EPYC Server*	*VTL-1* memory write
FALLOUT-2	*EPYC Server*	Disable SMM protection
FALLOUT-3	*EPYC Server*	*VTL-1* memory read *SMM* memory read (requires *FALLOUT-2*)

CHIMERA: Backdoors Inside Ryzen Chipset

The CHIMERA vulnerabilities are an array of hidden manufacturer backdoors inside *AMD's Promontory chipsets*. These chipsets are an integral part of all *Ryzen* and *Ryzen Pro* workstations. There exist two sets of backdoors, differentiated by their implementation: one is implemented within the firmware running on the chip, while the other is inside the chip's ASIC hardware. Because the latter has been manufactured into the chip, a direct fix may not be possible and the solution may involve either a workaround or a recall.

The backdoors outlined in this section provide multiple pathways for malicious code execution inside the chipset's internal processor. Because the chipset is a core system component, running malware inside the chip could have far reaching security implications.

The diagram below was taken from the instruction manual of *ASUS Crosshair VI Hero* Ryzen motherboard. It can be seen that not only is the chipset connected to the computer's USB, SATA, and PCI-E ports, it is also linked to the computer's LAN, WiFi, and Bluetooth.



In our research we have been able to execute our own code inside the chipset, and then leverage the latter's *Direct Memory Access (DMA)* engine to manipulate the operating system running on the main processor. These two capabilities form the foundation for malware, and provide a proof-of-concept. We believe that with additional research a determined attacker may also be able to reach the following capabilities:

Key Logger – It may be possible to implement a stealthy key logger by listening to USB traffic that flows through the chipset.

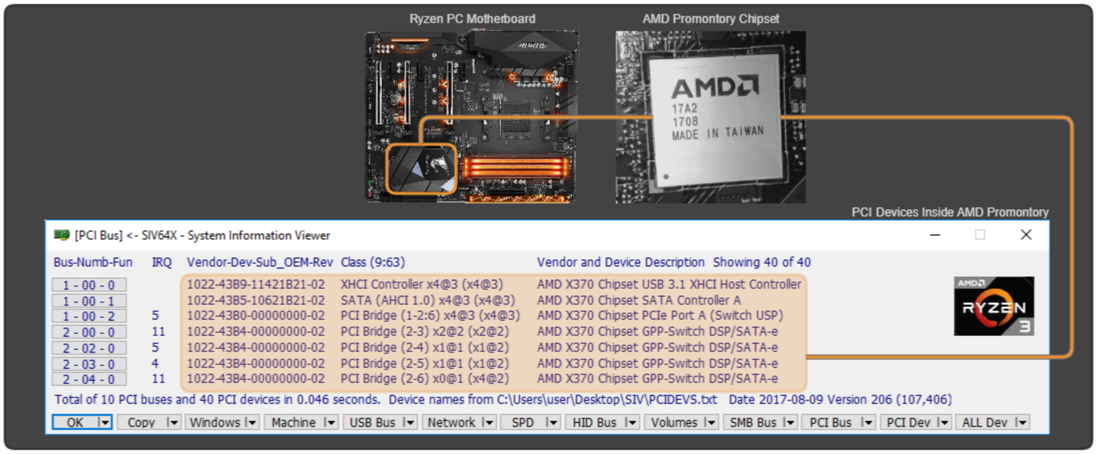
Network Access – It may be possible to implement network-based malware by leveraging the chipset's position as a middle-man for the machine's LAN, WiFi, and Bluetooth components.

Bypass Memory Protection – It may be possible to leverage the chipset's position to access protected memory areas such as *System Management RAM (SMRAM)*. We have verified this works on a small set of desktop motherboards.

Third-Party Chip Design Plagued with Hidden Backdoors

In November 2014, it was announced that AMD signed a contract with the Taiwanese chip manufacturer ASMedia, according to which ASMedia would design[12] AMD's chipset for the upcoming *Zen* processor series. This chipset, code-named *Promontory*, plays a central role within the company's latest generation *Ryzen* and *Ryzen Pro* workstations. It is responsible for linking the processor to external devices such as Hard Drives, USB devices, PCI Express cards, and occasionally also Network, Wi-Fi, and Bluetooth controllers.

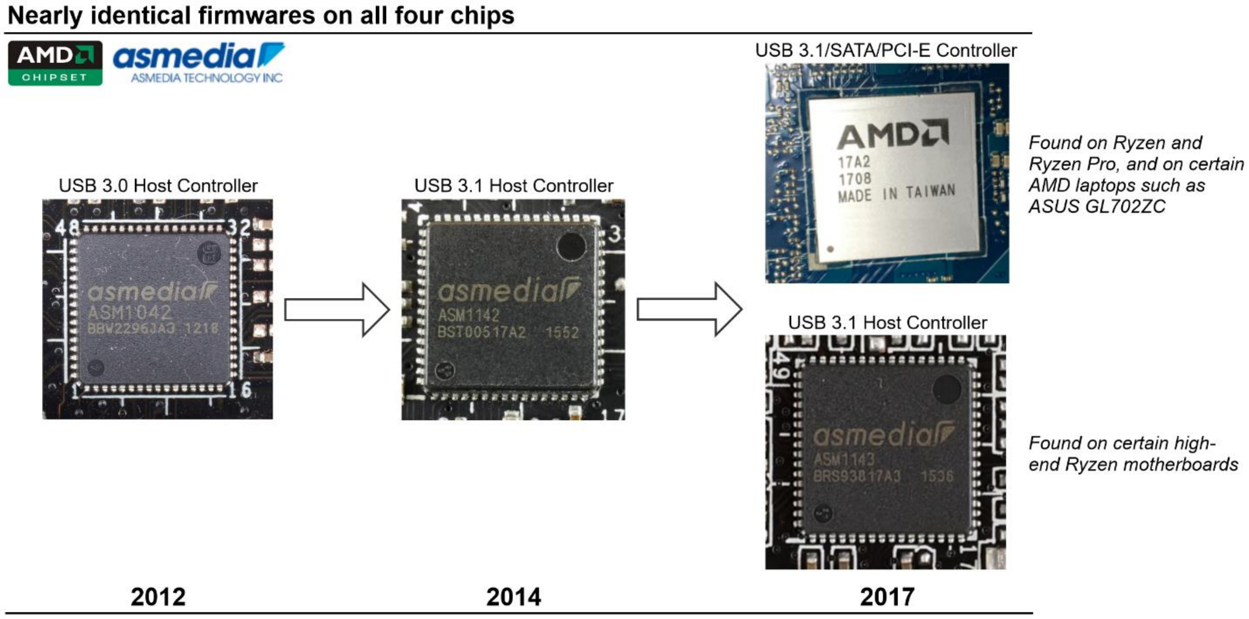
Although it is branded AMD, the Promontory chipset is not based on AMD technology. Rather, it is an amalgamation of several Integrated Circuits that ASMedia has been selling to OEMs for years, all merged together on a single silicon die. These integrated circuits are: (a) ASMedia USB host controller, known as ASM1142 or ASM1042, responsible for a workstation's USB ports; (b) ASMedia SATA controller, known as ASM1061, responsible for a workstation's hard drive and CD-ROM connections, and (c) ASMedia PCI-Express bridge controller, responsible for providing additional PCI-Express ports.



```
Bus-Numb-Fun  IRQ  Vendor-Dev-Sub_OEM-Rev  Class (9:63)                Vendor and Device Description  Showing 40 of 40
1 - 00 - 0         1022-43B9-11421B21-02   XHCI Controller x4@3 (x4@3)     AMD X370 Chipset USB 3.1 XHCI Host Controller
1 - 00 - 1         1022-43B5-10621B21-02   SATA (AHCI 1.0) x4@3 (x4@3)     AMD X370 Chipset SATA Controller A
1 - 00 - 2    5    1022-43B0-00000000-02   PCI Bridge (1-2:6) x4@3 (x4@3)  AMD X370 Chipset PCIe Port A (Switch USP)
2 - 00 - 0    11   1022-43B4-00000000-02   PCI Bridge (2-3) x2@2 (x2@2)    AMD X370 Chipset GPP-Switch DSP/SATA-e
2 - 02 - 0    5    1022-43B4-00000000-02   PCI Bridge (2-4) x1@1 (x1@2)    AMD X370 Chipset GPP-Switch DSP/SATA-e
2 - 03 - 0    4    1022-43B4-00000000-02   PCI Bridge (2-5) x1@1 (x1@2)    AMD X370 Chipset GPP-Switch DSP/SATA-e
2 - 04 - 0    11   1022-43B4-00000000-02   PCI Bridge (2-6) x0@1 (x4@2)    AMD X370 Chipset GPP-Switch DSP/SATA-e
Total of 10 PCI buses and 40 PCI devices in 0.046 seconds.  Device names from C:\Users\user\Desktop\SIV\PCIDEVS.txt  Date 2017-08-09 Version 206 (107,406)
```

The *Promontory* chipset is powered by an internal microcontroller that manages the chip's various hardware peripherals. Its built-in USB controller is primarily based on *ASMedia ASM1142*, which in turn is based on the company's older *ASM1042*. In our assessment, these controllers, which are commonly found on motherboards made by Taiwanese OEMs, have sub-standard security and no mitigations against exploitation. They are plagued with security vulnerabilities in both firmware and hardware, allowing attackers to run arbitrary code inside the chip, or to re-flash the chip with persistent malware. This, in turn, could allow for firmware-based malware that has full control over the system, yet is notoriously difficult to detect or remove. Such malware could manipulate the operating system through *Direct Memory Access (DMA)*, while remaining resilient against most endpoint security products.

[12] https://www.kitguru.net/components/cpu/anton-shilov/amd-and-asmedia-formally-sign-chipset-development-outsourcing-deal-report/


Nearly identical firmwares on all four chips
AMD CHIPSET
asmedia ASMEDIA TECHNOLOGY INC
USB 3.0 Host Controller
USB 3.1 Host Controller
USB 3.1/SATA/PCI-E Controller
USB 3.1 Host Controller
2012
2014
2017

Found on Ryzen and Ryzen Pro, and on certain AMD laptops such as ASUS GL702ZC

Found on certain high-end Ryzen motherboards

Our analysis suggests that *AMD Promontory* is heavily based on the design of *ASMedia ASM1142*. A comparison of the firmwares has shown that, during development, massive amounts of code were copied over from *ASM1142* into *AMD Promontory*, transferring many security vulnerabilities into AMD's *Ryzen* chipset.

Prerequisites for Exploitation

A program running with local-machine elevated administrator privileges. Access to the device is provided by a driver that is digitally signed by the vendor.

Affected Processors

Vulnerability	Affected Processors	Impact
CHIMERA-FW	*Ryzen* *Ryzen Pro*	Chipset code execution
CHIMERA-HW	*Ryzen* *Ryzen Pro*	Chipset code execution

Mitigations

No mitigations available. For the ASIC backdoors the issue could not be directly resolved, and the solution may involve either a workaround or a recall.

Conclusion

In this paper, we have summarized our findings concerning multiple vulnerabilities in AMD *Zen Architecture* processors. We believe that these vulnerabilities put networks that contain AMD computers at a considerable risk. Several of them open the door to malware that may survive computer reboots and reinstallations of the operating system, while remaining virtually undetectable by most endpoint security solutions. This can allow attackers to bury themselves deep within the computer system and to potentially engage in persistent, virtually undetectable espionage, executed from AMD's *Secure Processor* and AMD's chipset.

It is our view that the existence of these vulnerabilities betrays disregard of fundamental security principles. We hope that the security community takes note of these findings.

Important Legal Disclaimer

CTS is a research organization. This White Paper is intended for general information and educational purposes. This White Paper does not offer the reader any recommendations or professional advice. The opinions expressed in this report are not investment advice nor should they be construed as investment advice or any recommendation of any kind.

It summarizes security vulnerabilities, but purposefully does not provide a complete description of such vulnerabilities to protect users, such that a person with malicious intent could not actually exploit the vulnerabilities and try to cause harm to any user of the products described herein. Do not attempt to exploit or otherwise take advantage of the security vulnerabilities described in the White Paper.

The report and all statements contained herein are opinions of CTS and are not statements of fact. To the best of our ability and belief, all information contained herein is accurate and reliable, and has been obtained from public sources we believe to be accurate and reliable. Our opinions are held in good faith, and we have based them upon publicly available facts and evidence collected and analyzed, which we set out in our research report to support our opinions. We conducted research and analysis based on public information in a manner that any person could have done if they had been interested in doing so. You can publicly access any piece of evidence cited in this report or that we relied on to write this report. Although we have a good faith belief in our analysis and believe it to be objective and unbiased, you are advised that we may have, either directly or indirectly, an economic interest in the performance of the securities of the companies whose products are the subject of our reports. Any other organizations named in this White Paper have not confirmed the accuracy or determined the adequacy of its contents.

You may republish this White Paper in whole or in part as long as CTS is clearly and visibly credited and appropriately cited, and as long as you do not edit content.

Although we strive for accuracy and completeness to support our opinions, and we have a good-faith belief in everything we write, all such information is presented "as is," without warranty of any kind– whether express or implied – and CTS does not accept responsibility for errors or omissions. CTS reserves the right to change the contents of this White Paper and the restrictions on its use, with or without notice, and CTS reserves the right to refrain from updating this White Paper even as it becomes outdated or inaccurate.