Back to Security Bulletins and Briefs ↵

Guest Memory Vulnerabilities

AMD ID: AMD-SB-7014
Potential Impact: Arbitrary Code Execution
Severity: High

Summary

Researchers from IOActive have reported that it may be possible for an attacker with ring 0 access to modify the configuration of System Management Mode (SMM) even when SMM Lock is enabled.

CVE Details

Refer to Glossary for explanation of terms

CVE	CVSS	CVE Description
CVE-2023-31315	7.5 (High) AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H	Improper validation in a model specific register (MSR) could allow a malicious program with ring0 access to modify SMM configuration while SMI lock is enabled, potentially leading to arbitrary code execution.

Affected Products and Mitigation

The Platform Initialization (PI) versions listed below have been or will be released to the Original Equipment Manufacturers (OEM) to mitigate these issues. Please refer to your OEM for the BIOS update specific to your product.

Data Center

1st Gen AMD EPYC™ Processors formerly codenamed "Naples"

AMD plans to release the Platform Initialization (PI) firmware version indicated below.

For some CVEs, there may be alternative mitigation options provided as noted in Mitigation Option 2, including microcode and/or other patches.

<table>
<tr><th colspan="2">CVE</th><th>Mitigation Option 1</th><th colspan="2">Mitigation Option 2</th></tr>
<tr><td>CVE-2023-31315</td><td>7.5 (High)</td><td>Platform Initialization (PI)(Requires FW flash)</td><td colspan="2">µcode (Hot loadable)</td></tr>
<tr><td>Code Name</td><td>CPUID</td><td rowspan="2">Naples PI 1.0.0.M (2024-06-06)</td><td colspan="2">Version</td></tr>
<tr><td>Naples</td><td>0x00800F12</td><td>0x0800126F</td><td>2024-05-03</td></tr>
</table>

2nd Gen AMD EPYC™ Processors formerly codenamed "Rome"

AMD plans to release the Platform Initialization (PI) firmware version indicated below.

For some CVEs, there may be alternative mitigation options provided as noted in Mitigation Option 2, including microcode and/or other patches.

CVE		Mitigation Option 1	Mitigation Option 2
CVE-2023-31315	7.5 (High)	**Platform Initialization (PI) (Requires FW flash)**	**µcode (Hot loadable)**

Code Name	CPUID	Rome PI 1.0.0.J (2024-06-20)	Version	
Rome	0x00830F10		0x0830107C	2024-05-03

3rd Gen AMD EPYC™ Processors formerly codenamed “Milan" and “Milan-X”

AMD plans to release the Platform Initialization (PI) firmware version indicated below.

For some CVEs, there may be alternative mitigation options provided as noted in Mitigation Option 2, including microcode and/or other patches.

CVE		Mitigation Option 1	Mitigation Option 2	
CVE-2023-31315	7.5 (High)	**Platform Initialization (PI) (Requires FW flash)**	**µcode (Hot loadable)**	
Code Name	**CPUID**	Milan PI 1.0.0.D (2024-07-11)	**Version**	
Milan	0x00A00F11		0x0A0011D5	2024-05-03
Milan-X	0x00A00F12		0x0A001238	

4th Gen AMD EPYC™ Processors formerly codenamed "Genoa", “Genoa-X”, “Bergamo”, and “Siena”

AMD recommends updating to the Platform Initialization (PI) firmware version indicated below.

For some CVEs, there may be alternative mitigation options provided as noted in Mitigation Option 2, including microcode and/or other patches.

CVE		Mitigation Option 1	Mitigation Option 2
CVE-2023-31315	7.5 (High)	**Platform Initialization**	**µcode (Hot loadable)**

		(PI) (Requires FW flash)		
Code Name	**CPUID**	Genoa PI 1.0.0.C (2024-04-04)	**Version**	
Genoa	0x00A10F11		0x0A101148	2024-05-03
Genoa-X	0x00A10F12		0x0A101248	
Bergamo/Siena	0x00AA0F02		0x0AA00215	

DATA CENTER GRAPHICS

CVE	**AMD Instinct™ MI300A**
CVE-2023-31315	MI300 SR5 PI1.0.0.2 (2024-05-15)

EMBEDDED PROCESSORS

CVE	**AMD EPYC™ Embedded 3000**	**AMD EPYC™ Embedded 7002**	**AMD EPYC™ Embedded 7003**	**AMD EPYC™ Embed 9003**
CVE-2023-31315	SnowyOwlPI 1.1.0.D (Target Oct 2024)	EmbRomePI-SP3 1.0.0.C (Target Oct 2024)	EmbMilanPI-SP3 1.0.0.9 (Target Oct 2024)	EmbGenoaPI 1.0.0.7 (2024-0 15)

CVE	**AMD Ryzen™ Embedded R1000**	**AMD Ryzen™ Embedded R2000**	**AMD Ryzen™ Embedded 5000**	**AMD Ryze 7000**
CVE-2023-31315	EmbeddedPI-FP5 1.2.0.D (Target Oct 2024)	EmbeddedR2KPI-FP5 1.0.0.4 (Target Oct 2024)	EmbAM4PI 1.0.0.6 (Target Oct 2024)	Emb 1.0.0 (Targ

CVE	AMD Ryzen™ Embedded V1000		AMD Ryzen™ Embedded V2000	AMD Ryzen™ Er V3000
	All V1000 OPNs excluding YE1500C4T4MFH	YE1500C4T4MFH		
CVE-2023-31315	TBD (Target Oct 2024)		EmbeddedPI-FP6 1.0.0.A (Target Oct 2024)	Embedded 1.0.0.B (Target Oc

CLIENT

DESKTOP

CVE	AMD Ryzen™ 3000 Series Desktop Processors (Formerly codenamed) “Matisse”	AMD Ryzen™ 5000 Series Desktop Processors (Formerly codenamed) “Vermeer”	AMD Ryzen™ 5000 Series Desktop processor with Radeon™ Graphics (Formerly codenamed) “Cezanne”	AMD Ryzen™ 7000 Series Desktop Processors (Formerly codenamed) “Raphael” X3D
CVE-2023-31315	No fix planned	ComboAM4v2PI 1.2.0.cb (2024-07-30)	ComboAM4v2PI 1.2.0.cb (2024-07-30)	ComboAM5PI 1.2.0.1 (2024-08-07)

CVE	AMD Ryzen™ 4000 Series Desktop Processors with Radeon™ Graphics (Formerly codenamed) “Renoir” AM4	AMD Ryzen™ 8000 Series Processors with Radeon™ Graphics (Formerly codenamed) “Phoenix” AM5
CVE-2023-31315	ComboAM4v2PI 1.2.0.cb (2024-07-30)	ComboAM5PI 1.2.0.1 (2024-08-07)

HIGH END DESKTOP (HEDT)

CVE	AMD Ryzen™ Threadripper™ 3000 Series	AMD Ryzen™ Threadripper™ 7000

	Processors (Formerly codenamed) “Castle Peak” HEDT	**Series Processors (Formerly codenamed) “Storm Peak”**
CVE-2023-31315	CastlePeakPI-SP3r3 1.0.0.B (2024-07-25)	StormPeakPI-SP6 1.1.0.0f (2024-05-23) StormPeakPI-SP6 1.0.0.1h (2024-05-30)

WORKSTATION

CVE	**AMD Ryzen™ Threadripper™ PRO Processors (Formerly codenamed) “Castle Peak” WS SP3**	**AMD Ryzen™ Threadripper™ PRO 3000WX Series Processors (Formerly codenamed) “Chagall” WS**
CVE-2023-31315	ChagallWSPI-sWRX8 1.0.0.8 (2024-07-22) CastlePeakWSPI-sWRX8 1.0.0.D (2024-07-26)	ChagallWSPI-sWRX8 1.0.0.8 (2024-07-22)

MOBILE - AMD Athlon™ Series Processors

CVE	**AMD Athlon™ 3000 Series Mobile Processors with Radeon™ Graphics (Formerly codenamed) “Dali”/”Dali” ULP**	**AMD Athlon™ 3000 Series Mobile Processors with Radeon™ Graphics (Formerly codenamed) “Pollock”**
CVE-2023-31315	Picasso-FP5 1.0.1.2 (2024-08-06)	PollockPI-FT5 1.0.0.8 (2024-08-06)

MOBILE - AMD Ryzen™ Series Processors

CVE	AMD Ryzen™ 3000 Series Mobile Processor with Radeon™ Graphics (Formerly codenamed) “Picasso” FP5	AMD Ryzen™ 4000 Series Mobile Processors with Radeon™ Graphics (Formerly codenamed) “Renoir” FP6	AMD Ryzen™ 5000 Series Mobile Processors with Radeon™ Graphics (Formerly codenamed) “Lucienne”	AMD Ryzen™ 5000 Series Mobile Processors with Radeon™ Graphics (Formerly codenamed) “Cezanne”	AMD Ryz 7020 Ser Processo with Radeon Graphics (Former codenam “Mendoc FT6
CVE-2023-31315	Picasso-FP5 1.0.1.2 (2024-08-06)	RenoirPI-FP6 1.0.0.E (2024-08-07)	CezannePI-FP6 1.0.1.1 (2024-07-31)	CezannePI-FP6 1.0.1.1 (2024-07-31)	Mendoci FT6 1.0.0.7 (2024-08

CVE	AMD Ryzen™ 6000 Series Processors with Radeon™ Graphics (Formerly codenamed) "Rembrandt"	AMD Ryzen™ 7035 Series Processors with Radeon™ Graphics (Formerly codenamed) “Rembrandt-R”	AMD Ryzen™ 5000 Series Processors with Radeon™ Graphics (Formerly codenamed) “Barcelo”	AMD Ryzen™ 7030 Series Mobile Processors with Radeon™ Graphics (Formerly codenamed) “Barcelo-R”	AMD R 7040 Se Mobile Proces with Ra Graphi (Forme codena “Phoen FP7/FP
CVE-2023-31315	RembrandtPI-FP7 1.0.0.B (2024-07-03)	RembrandtPI-FP7 1.0.0.B (2024-07-03)	CezannePI-FP6 1.0.1.1 (2024-07-31)	CezannePI-FP6 1.0.1.1 (2024-07-31)	Phoeni FP7 1.1 (2024-0

Acknowledgement

AMD thanks Enrique Nissim and Krzysztof Okupski of IOActive for reporting this issue and engaging in coordinated vulnerability disclosure.

Revisions

Revision Date	Description
2024-08-09	Initial publication

DISCLAIMER

The information contained herein is for informational purposes only and is subject to change without notice. While every precaution has been taken in the preparation of this document, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of this document, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. Any computer system has risks of security vulnerabilities that cannot be completely prevented or mitigated. No license, including implied or arising by estoppel, to any intellectual property rights is granted by this document. Terms and limitations applicable to the purchase or use of AMD’s products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale.

AMD, the AMD Arrow logo, EPYC, Instinct, Radeon, Ryzen, Threadripper and combinations thereof are trademarks of Advanced Micro Devices, Inc. CVE and the CVE logo are registered trademarks of The MITRE Corporation. Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

Third party content may be licensed to you directly by the third party that owns the content and is not licensed to you by AMD. ALL LINKED THIRD-PARTY CONTENT IS PROVIDED ‘AS IS’ WITHOUT A WARRANTY OF ANY KIND. USE OF SUCH THIRD-PARTY CONTENT IS DONE AT YOUR SOLE DISCRETION AND UNDER NO CIRCUMSTANCES WILL AMD BE LIABLE TO YOU FOR ANY THIRD-PARTY CONTENT. YOU ASSUME ALL RISK AND ARE SOLELY RESPONSIBILITY FOR ANY DAMAGES THAT MAY ARISE FROM YOUR USE OF THIRD-PARTY CONTENT.

Subscribe to the latest news from AMD

Company

About AMD

Management Team

Corporate Responsibility

Careers

Contact Us

News & Events

Newsroom

Events

Blogs

Media Library

Community

Support

Developer

Red Team

Partners

Developer Central

AMD Partner Hub

Partner Resource Library

Authorized Distributors

AMD University Program

Investors