



CVE-2022-42336

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-42336
State	PUBLIC
Assigner	security@xen.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-17 01:15:00 UTC
Updated	2023-11-07 03:53:00 UTC
Description	Mishandling of guest SSBD selection on AMD hardware The current logic to set SSBD on AMD Family 17h and Hygon Far

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	4.17	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 38 Update: xen-4.17.1-2.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 38 Update: xen-4.17.1-2.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
xenbits.xenproject.org/xsa/advisory-431.txt	MISC	xenbits.xenproject.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[182265](#) Debian Security Update for xen (CVE-2022-42336)

[284133](#) Fedora Security Update for xen (FEDORA-2023-8334fe0ecb)

[503146](#) Alpine Linux Security Update for xen

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)