



CVE-2022-23005

Published on: Not Yet Published

Last Modified on: 01/24/2023 02:40:00 PM UTC

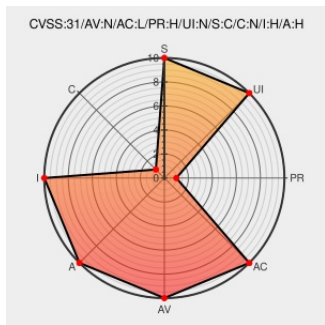
CVE-2022-23005

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of **NA** from **NA** contain the following vulnerability:

Western Digital has identified a weakness in the UFS standard that could result in a security vulnerability. This vulnerability may exist in some systems where the Host boot ROM code implements the UFS Boot feature to boot from UFS compliant storage devices. The UFS Boot feature, as specified in the UFS standard, is provided by UFS devices to support platforms that need to download the system boot loader from external non-volatile storage locations. Several scenarios have been identified in which adversaries may disable the boot capability, or revert to an old boot loader code, if the host boot ROM code is improperly implemented. UFS Host Boot ROM implementers may be impacted by this vulnerability. UFS devices are only impacted when connected to a vulnerable UFS Host and are not independently impacted by this vulnerability. When present, the vulnerability is in the UFS Host implementation and is not a vulnerability in Western Digital UFS Devices. Western Digital has provided details of the vulnerability to the JEDEC standards body, multiple vendors of host processors, and software solutions providers.

Several scenarios have been identified in which adversaries may disable the boot capability, or revert to an old boot loader code, if the host boot ROM code is improperly implemented. UFS Host Boot ROM implementers may be impacted by this vulnerability. UFS devices are only impacted when connected to a vulnerable UFS Host and are not independently impacted by this vulnerability. When present, the vulnerability is in the UFS Host implementation and is not a vulnerability in Western Digital UFS Devices. Western Digital has provided details of the vulnerability to the JEDEC standards body, multiple vendors of host processors, and software solutions providers.

CVE-2022-23005 has been assigned by psirt@wdc.com to track the vulnerability

Affected Vendor/Software: **NA** - **NA** version **NA**

CVE References

Description	Tags	Link
	documents.westerndigital.com application/pdf	MISC documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-host-boot-rom-code-vulnerability-and-mitigation.pdf
WDC-23001 Host Boot ROM Code Vulnerability in Systems Implementing UFS Boot Feature Western Digital	www.westerndigital.com text/html	MISC www.westerndigital.com/support/product-security/wdc-23001-host-boot-rom-code-vulnerability-in-systems-implementing-ufs-boot-feature

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Western Digital has identified a weakness in the UFS standard that could result in a security vulnerability. This vul...

Known Affected Software

Vendor	Product	Version
NA	NA	NA

Discovery Credit

Rotem Sela and Avri Altman of Western Digital

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-23005 : Western Digital has identified a weakness in the UFS standard that could result in a security vuln... twitter.com/i/web/status/1...	2023-01-23 22:05:55
 /r/netcve	CVE-2022-23005	2023-01-23 22:38:20

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status status.cve.report