

# Public Security Advisory

Solidigm Product Security Incident Response Team

**Title:** Solidigm™ SSD Firmware Advisory

**Solidigm ID:** SOLIDIGM-SA-00563 rev 1.1

**Advisory Category:** Public Security Advisory

**Impact of Vulnerability:** Escalation of Privilege, Denial of Service, Information Disclosure

## Summary:

Potential security vulnerabilities in some Solidigm™ (Formerly Intel®) SSD products may allow escalation of privilege, denial of service or information disclosure. Solidigm is releasing firmware updates and prescriptive guidance to mitigate these potential vulnerabilities.

## Vulnerabilities:

CVEID: [CVE-2021-33069](#)

CVSS Base Score: 6.0 Medium

CVSS Vector: [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H](#)

CVEID: [CVE-2021-33074](#)

CVSS Base Score: 6.8 Medium

CVSS Vector: [CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N](#)

CVEID: [CVE-2021-33075](#)

CVSS Base Score: 6.0 Medium

CVSS Vector: [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H](#)

CVEID: [CVE2021-33076](#)

CVSS Base Score: 5.3 Medium

CVSS Vector: [CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N](#)

CVEID: [CVE-2021-33077](#)

CVSS Base Score: 7.3 High  
CVSS Vector: [CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N](#)

CVEID: [CVE-2021-33078](#)  
CVSS Base Score: 7.9 High  
CVSS Vector: [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:H](#)

CVEID: [CVE-2021-33079](#)  
CVSS Base Score: 4.1 Medium  
CVSS Vector: [CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N](#)

CVEID: [CVE-2021-33080](#)  
CVSS Base Score: 7.3 High  
CVSS Vector: [CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N](#)

CVEID: [CVE-2021-33081](#)  
CVSS Base Score: 7.9 High  
CVSS Vector: [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:H](#)

CVEID: [CVE-2021-33082](#)  
CVSS Base Score: 5.3 Medium  
CVSS Vector: [CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N](#)

CVEID: [CVE-2021-33083](#)  
CVSS Base Score: 6.0 Medium  
CVSS Vector: [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H](#)

## Affected Products & Recommendations

<b>Product Family (all formerly Intel®)</b>	<b>Mitigated Version or higher</b>
<b>Solidigm™ SSD DC P4500</b> <b>Solidigm™ SSD DC P4501</b> <b>Solidigm™ SSD DC P4600</b> <b>Solidigm™ SSD DC P4608</b>	QDV101B1
<b>Solidigm™ SSD DC P4511 Series (M.2 w/Opal)</b>	VCV1MD1A or VDC1LZ37
<b>Solidigm™ SSD DC P4511 Series (EDSFF w/Opal)</b> <b>Solidigm™ SSD DC P4510 Series (EDSSF w/Opal)</b>	VEV10284
<b>Solidigm™ SSD DC P4510 Series (SFF w/Opal)</b> <b>Solidigm™ SSD DC P4610 Series (SFF w/Opal)</b>	VDV10184
<b>Solidigm™ SSD DC D4512</b>	VPV1ET0K
<b>Solidigm™ SSD D5 P4316 (Opal)</b>	8DV1MD58
<b>Solidigm™ SSD D3-S4510 Series (SFF)</b> <b>Solidigm™ SSD D3-S4610 Series (SFF)</b>	XCV10132
<b>Solidigm™ SSD D3-S4510 Series (M.2)</b> <b>Solidigm™ SSD D3-S4610 Series (M.2)</b>	XC311132
<b>Solidigm™ SSD D7 P5500 Series</b> <b>Solidigm™ SSD D7 P5600 Series</b>	2CV1R200, 2CV1C030, 1.1.5
<b>Solidigm™ SSD D7 P5510 Series (Opal)</b>	JCV10200
<b>Solidigm™ SSD D5-P5316 Series</b>	ACV10200
<b>Solidigm™ SSD DC P3100 Series</b>	119D
<b>Solidigm™ SSD DC S4500 Series</b> <b>Solidigm™ SSD DC S4600 Series</b>	SCV10150
<b>Solidigm™ SSD 600p Series</b>	122C
<b>Solidigm™ SSD 660p Series</b>	005C <sup>1</sup>
<b>Solidigm™ SSD 665p Series</b>	002C <sup>1</sup>
<b>Solidigm™ SSD 670p Series</b>	003C
<b>Solidigm™ SSD 700p Series</b>	005C <sup>1</sup>
<b>Solidigm™ SSD 760p Series</b>	006C <sup>1</sup>
<b>Solidigm™ SSD Pro 7600p Series</b>	006P <sup>1</sup>
<b>Solidigm™ SSD E 6000p Series</b>	122E
<b>Solidigm™ SSD Pro 6000p Series</b>	132P

<b>Solidigm™ SSD E 6100p Series</b>	006E <sup>1</sup>
<b>Solidigm™ SSD DC P3100 Series</b>	119D
<b>Solidigm™ SSD DC P4101 Series</b>	009D <sup>1</sup>

Footnote: 1. Consult prescriptive guidance below concerning CVE-2021-33082

Solidigm recommends to always use the latest available Firmware

Updates are available for download at this location: [Solidigm Storage Tool](#)

Prescriptive guidance for CVE-2021-33082: Two possible workarounds is to use one of the following commands listed below instead of the Sanitize command with Block Erase operation:

- NVMe Sanitize command, Crypto Erase (SANACT=04h)
- NVMe Format NVM command, User Data Erase or Crypto Erase (SES=01h or SES=02h)

Check the Identify Controller Data Structure below, for capability your drive supports in lieu of Sanitize erase feature:

- Sanitize command, Crypto Erase (offset 331:328, SANICAP bit 00h)
- NVMe Format NVM command (offset 257:256, OACS bit 01h)

## Acknowledgements:

These issues were found internally by Intel® and/or Solidigm.

Solidigm, and nearly the entire technology industry, follows a disclosure practice called Coordinated Disclosure, under which a cybersecurity vulnerability is generally publicly disclosed only after mitigations are available.

Effective December 29<sup>th</sup>, 2021, all listed Solidigm™ SSDs (formerly Intel®) affected products are supported solely by Solidigm.

Any update to this communication will be available for download at this location: <https://www.solidigm.com/en/support.html>

For affected Intel® Optane™ products, Solidigm recommends customers consult Intel® Security Advisory published at: <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00563.html>

## Revision history:

Revision	Date	Description
1.0	05/11/2022	Initial Release
1.1	06/17/2022	<ul style="list-style-type: none"><li>• Solidigm™ SSD D5-P5326 Series typo fixed and replaced by Solidigm™ SSD D5-P5316</li><li>• Added Solidigm™ SSD Pro 6000p Series</li><li>• Added Solidigm™ SSD DC P4500</li><li>• Added Solidigm™ SSD DC P4501</li><li>• Added Solidigm™ SSD DC P4600</li><li>• Added Solidigm™ SSD DC P4608</li><li>• Added Solidigm™ SSD DC D4512</li><li>• Added Solidigm™ SSD DC P4510 Series (EDSSF w/Opal)</li><li>• Added Solidigm™ SSD DC P4510 Series (SFF w/Opal)</li></ul>

## Embargo:

The information in this Public Security Advisory is subject to public embargo until 10 a.m. (UTC -7) on 05/10/2022 ("Embargo"). This information may not be disclosed until after the Embargo without permission.

Intel® and Intel® Optane™ are registered trademarks of Intel Corporation.