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

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

Solidigm™ SSD E 6100p Series	006E[1]
Solidigm™ SSD DC P3100 Series	119D
Solidigm™ SSD DC P4101 Series	009D[1]

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 29th, 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	• Solidigm™ SSD D5-P5326 Series typo fixed and replaced by Solidigm™ SSD D5-P5316 • Added Solidigm™ SSD Pro 6000p Series • Added Solidigm™ SSD DC P4500 • Added Solidigm™ SSD DC P4501 • Added Solidigm™ SSD DC P4600 • Added Solidigm™ SSD DC P4608 • Added Solidigm™ SSD DC D4512 • Added Solidigm™ SSD DC P4510 Series (EDSSF w/Opal) • Added Solidigm™ SSD DC P4510 Series (SFF w/Opal)

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.