



CVE-2020-24055

Published on: 08/21/2020 12:00:00 AM UTC

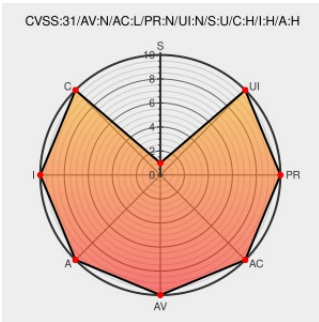
Last Modified on: 03/23/2021 11:23:36 PM UTC

CVE-2020-24055

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [4320](#) from [Verint](#) contain the following vulnerability: Verint 5620PTZ Verint_FW_0_42 and Verint 4320 V4320_FW_0_23, and V4320_FW_0_31 units feature an autodiscovery service implemented in the binary executable '/usr/sbin/DM' that listens on port TCP 6666. The service is vulnerable to a stack buffer overflow. It is worth noting that this service does not require any authentication.

CVE-2020-24055 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|------------------|------------------------|---------------------|---------------------|
| NETWORK | LOW | NONE | NONE |
| Scope | Confidentiality Impact | Integrity Impact | Availability Impact |
| UNCHANGED | HIGH | HIGH | HIGH |

CVSS2 Score: **7.5 - HIGH**

| Access Vector | Access Complexity | Authentication |
|------------------------|-------------------|---------------------|
| NETWORK | LOW | NONE |
| Confidentiality Impact | Integrity Impact | Availability Impact |
| PARTIAL | PARTIAL | PARTIAL |

CVE References

| Description | Tags | Link |
|--|---|--|
| Verint PTZ Cameras Multiple Vulnerabilities IOActive | Third Party Advisory ioactive.com text/html | MISC ioactive.com/verint-ptz-cameras-multiple-vulnerabilities/ |
| No Description Provided | Exploit | MISC ioac.tv/2Nbc40h |

Third Party Advisory

ioac.tv

text/html

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

Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|------------------------|----------------------------------|----------------|--------|---------|----------|
| Hardware | Verint | 4320 | - | All | All | All |
| Hardware | Verint | 4320 | - | All | All | All |
| Operating System | Verint | 4320 Firmware | v4320_fw_0_23 | All | All | All |
| Operating System | Verint | 4320 Firmware | v4320_fw_0_31 | All | All | All |
| Operating System | Verint | 4320 Firmware | v4320_fw_0_23 | All | All | All |
| Operating System | Verint | 4320 Firmware | v4320_fw_0_31 | All | All | All |
| Hardware | Verint | 5620ptz | - | All | All | All |
| Hardware | Verint | 5620ptz | - | All | All | All |
| Operating System | Verint | 5620ptz Firmware | verint_fw_0_42 | All | All | All |
| Operating System | Verint | 5620ptz Firmware | verint_fw_0_42 | All | All | All |

cpe:2.3:h:verint:4320:-:*:*:*:*:*:

cpe:2.3:h:verint:4320:-:*:*:*:*:*:

cpe:2.3:o:verint:4320_firmware:v4320_fw_0_23:*:*:*:*:*:

cpe:2.3:o:verint:4320_firmware:v4320_fw_0_31:*:*:*:*:*:

cpe:2.3:o:verint:4320_firmware:v4320_fw_0_23:*:*:*:*:*:

cpe:2.3:o:verint:4320_firmware:v4320_fw_0_31:*:*:*:*:*:

cpe:2.3:h:verint:5620ptz:-:*:*:*:*:*:

cpe:2.3:h:verint:5620ptz:-:*:*:*:*:*:

cpe:2.3:o:verint:5620ptz_firmware:verint_fw_0_42:*:*:*:*:*:

cpe:2.3:o:verint:5620ptz_firmware:verint_fw_0_42:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2022   |

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](#)