



# CVE-2017-16674

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

## Summary

|                 |                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2017-16674                                                                                                     |
| State           | PUBLISHED                                                                                                          |
| Assigner        | mitre                                                                                                              |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                       |
| Published       | 2017-11-09 04:29:00 UTC                                                                                            |
| Updated         | 2025-04-20 01:37:25 UTC                                                                                            |
| Description     | Datto Windows Agent allows unauthenticated remote command execution via a modified command in conjunction with CVE |

## Risk And Classification

Primary CVSS: v3.0 8 HIGH from nvd@nist.gov

CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Problem Types: NVD-CWE-noinfo | n/a

| Version | Source       | Type    | Score | Severity | Vector                                       |
|---------|--------------|---------|-------|----------|----------------------------------------------|
| 3.0     | nvd@nist.gov | Primary | 8     | HIGH     | CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H |
| 2.0     | nvd@nist.gov | Primary | 4.9   |          | AV:A/AC:M/Au:S/C:P/I:P/A:P                   |

## CVSS v3.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

Medium

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:A/AC:M/Au:S/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product       | Version | Update | Edition | Language |
|-------------|--------|---------------|---------|--------|---------|----------|
| Application | Datto  | Windows Agent | All     | All    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor | Product | Version      | Platforms     |
|--------|--------|---------|--------------|---------------|
| CNA    | Na     | N/a     | affected n/a | Not specified |

References

| Reference                                                                             | Source                               | Link                        |
|---------------------------------------------------------------------------------------|--------------------------------------|-----------------------------|
| Open letter to Datto partners regarding two reported product security vulnerabilities | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.datto</a>   |
| CVE Program record                                                                    | CVE.ORG                              | <a href="#">www.cve.o</a>   |
| NVD vulnerability detail                                                              | NVD                                  | <a href="#">nvd.nist.go</a> |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)