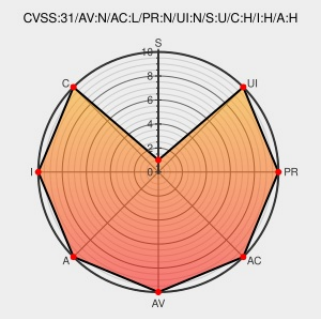
# CVE-2021-20204

Published on: 05/06/2021 12:00:00 AM UTC

Last Modified on: 02/12/2023 10:15:00 PM UTC

## CVE-2021-20204

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Debian Linux from Debian contain the following vulnerability:

A heap memory corruption problem (use after free) can be triggered in libgetdata v0.10.0 when processing maliciously crafted dirfile databases. This degrades the confidentiality, integrity and availability of third-party software that uses libgetdata as a library. This vulnerability may lead to arbitrary code execution or privilege escalation depending on input/skills of attacker.

CVE-2021-20204 has been assigned by secalert@redhat.com 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 |
|---|---|---|
| [SECURITY] Fedora 34 | lists.fedoraproject.org text/html | MISC lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/GB7T7DW7XRPJOUE25ZE7GF244FPCHBWY/ |

| | | |
|---|---|---|
| Update: getdata-0.11.0-1.fc34 - package-announce - Fedora Mailing-Lists | | |
| [SECURITY] Fedora 33 Update: getdata-0.11.0-1.fc33 - package-announce - Fedora Mailing-Lists | lists.fedoraproject.org text/html | MISC lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/43JTGEMYMCTHD3LHFD7ENBNSWCNBCYEY/ |
| [SECURITY] Fedora 35 Update: getdata-0.11.0-1.fc35 - package-announce - Fedora Mailing-Lists | lists.fedoraproject.org text/html | MISC lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/OE23HBLIVKVPOQ5MVADWPOCFMREVF4QZ/ |
| [SECURITY] [DLA 2660-1] libgetdata security update | lists.debian.org text/html | MLIST [debian-lts-announce] 20210513 [SECURITY] [DLA 2660-1] libgetdata security update |
| 1956348 – (CVE-2021-20204) CVE-2021-20204 getdata: Use after free in _GD_Supports() in encoding.c | bugzilla.redhat.com text/html | MISC bugzilla.redhat.com/show_bug.cgi?id=1956348 |



## Related QID Numbers

178592 Debian Security Update for libgetdata (DLA 2660-1)

180035 Debian Security Update for libgetdata (CVE-2021-20204)

282075 Fedora Security Update for getdata (FEDORA-2021-197545a753)

282076 Fedora Security Update for getdata (FEDORA-2021-3b8bb26909)

282150 Fedora Security Update for getdata (FEDORA-2021-e2b64c614b)

751570 OpenSUSE Security Update for getdata (openSUSE-SU-2021:1645-1)

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Fedoraproject | Fedora | 34 | All | All | All |
| Operating System | Fedoraproject | Fedora | 35 | All | All | All |
| Application | Getdata Project | Getdata | 0.10.0 | All | All | All |

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*:

cpe:2.3:a:getdata_project:getdata:0.10.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2021-20204 : A heap memory corruption problem use after free can be triggered in libgetdata v0.10.0 when proc… twitter.com/i/web/status/1… | 2021-05-06 15:03:25 |
| /r/netcve | CVE-2021-20204 | 2021-05-06 15:43:57 |

← Previous ID

Next ID→