



# HNB Organizer 1.9.18-10 Local Buffer Overflow via -rc Parameter

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

## Summary

|                 |                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2016-20045                                                                                                                 |
| State           | PUBLISHED                                                                                                                      |
| Assigner        | VulnCheck                                                                                                                      |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                   |
| Published       | 2026-03-28 12:16:00 UTC                                                                                                        |
| Updated         | 2026-04-08 20:41:56 UTC                                                                                                        |
| Description     | HNB Organizer 1.9.18-10 contains a local buffer overflow vulnerability that allows local attackers to execute arbitrary code t |

## Risk And Classification

Primary CVSS: v4.0 8.6 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000150000 probability, percentile 0.032420000 (date 2026-04-13)

Problem Types: CWE-787 | CWE-787 Out-of-bounds Write

| Version | Source                   | Type      | Score | Severity | Vector                                                        |
|---------|--------------------------|-----------|-------|----------|---------------------------------------------------------------|
| 4.0     | disclosure@vulncheck.com | Secondary | 8.6   | HIGH     | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA |
| 4.0     | CNA                      | CVSS      | 8.6   | HIGH     | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA |
| 3.1     | nvd@nist.gov             | Primary   | 7.8   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H                  |
| 3.1     | disclosure@vulncheck.com | Secondary | 8.4   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H                  |
| 3.1     | CNA                      | CVSS      | 8.4   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H                  |

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X



CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor      | Product               | Version | Update | Edition | Language |
|-------------|-------------|-----------------------|---------|--------|---------|----------|
| Application | Hnb Project | Hierarchical Notebook | All     | All    | All     | All      |

Vendor Declared Affected Products

| Vendor Declared Affected Products                                                  |                          |                     |                    |               |
|------------------------------------------------------------------------------------|--------------------------|---------------------|--------------------|---------------|
| Source                                                                             | Vendor                   | Product             | Version            | Platforms     |
| CNA                                                                                | Hnb                      | HNB                 | affected 1.9.18-10 | Not specified |
|                                                                                    |                          |                     |                    |               |
| References                                                                         |                          |                     |                    |               |
| Reference                                                                          | Source                   | Link                | Ta                 |               |
| hnb.sourceforge.net                                                                | disclosure@vulncheck.com | hnb.sourceforge.net | Pr                 |               |
| www.vulncheck.com/advisories/hnb-organizer-10-local-buffer-overflow-via-rc-para... | disclosure@vulncheck.com | www.vulncheck.com   | Th                 |               |
| www.exploit-db.com/exploits/40025                                                  | disclosure@vulncheck.com | www.exploit-db.com  | Ex                 |               |
| CVE Program record                                                                 | CVE.ORG                  | www.cve.org         | ca                 |               |
| NVD vulnerability detail                                                           | NVD                      | nvd.nist.gov        | ca                 |               |
| <div><div></div><div></div></div>                                                  |                          |                     |                    |               |
| Vendor Comments And Credit                                                         |                          |                     |                    |               |
| Discovery Credit                                                                   |                          |                     |                    |               |
| <b>CNA:</b> Juan Sacco - http://www.exploitpack.com - jsacco@exploitpack.com (en)  |                          |                     |                    |               |
|                                                                                    |                          |                     |                    |               |
| There are currently no legacy QID mappings associated with this CVE.               |                          |                     |                    |               |