



WordPress Simple History Plugin <= 3.3.1 is vulnerable to CSV Injection

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2022-45350 |
| State | PUBLISHED |
| Assigner | Patchstack |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-11-07 15:15:09 UTC |
| Updated | 2026-04-28 19:18:58 UTC |
| Description | Improper Neutralization of Formula Elements in a CSV File vulnerability in Pär Thernström Simple History – user activity log |

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

Problem Types: CWE-1236 | CWE-1236 CWE-1236 Improper Neutralization of Formula Elements in a CSV File

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | ADP | DECLARED | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | audit@patchstack.com | Secondary | 5.8 | MEDIUM | CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:N/I:H/A:N |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 3 | LOW | CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:N/I:H/A:N |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------------------------------|--------------------------------|---------|--------|---------|----------|
| Application | Simple-history | Simple History | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|------------------------------|---|---------------------------|---------------|
| CNA | Pr Thernstrm | Simple History User Activity Log Audit Tool | affected n/a 3.3.1 custom | Not specified |

References

| Reference | Source | Link |
|---|--|---|
| WordPress Simple History plugin <= 3.3.1 - CSV Injection vulnerability - Patchstack | af854a3a-2127-422b-91ae-364da2661108 | patchstack.com/database/Wordpress/Plugin/simple-history/vulnerability/wordpr... |
| patchstack.com/database/Wordpress/Plugin/simple-history/vulnerability/wordpr... | MITRE | patchstack.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

Vendor Comments And Credit

Discovery Credit

CNA: [ed32.dll \(Patchstack\)](#) (en)

Additional Advisory Data

Solutions

CNA: Update to 3.4.0 or a higher version.

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

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

CVE.report and Source URL Uptime Status status.cve.report