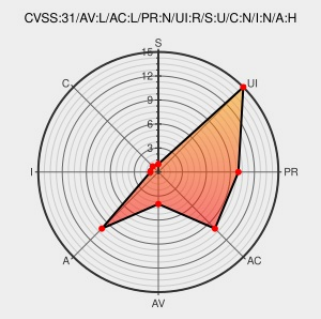
CVE-2019-19035

Published on: 11/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19035

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



Certain versions of Jhead from Jhead Project contain the following vulnerability:

jhead 3.03 is affected by: heap-based buffer over-read. The impact is: Denial of service. The component is: ReadJpegSections and process_SOFn in jpgfile.c. The attack vector is: Open a specially crafted JPEG file.

CVE-2019-19035 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] Fedora 31 Update: jhead-3.04-1.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-948e6ebaeb
[SECURITY] Fedora 30 Update: jhead-3.04-1.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-7efb86afdc

JHead: Multiple vulnerabilities (GLSA 202007-17) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202007-17
1765647 – Invalid read in function ReadJpegSections and process_SOFn	Exploit Issue Tracking Tool Signature bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1765647

Related QID Numbers

199359 Ubuntu Security Notification for Jhead Vulnerabilities (USN-6098-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jhead Project	Jhead	3.03	All	All	All
Application	Jhead Project	Jhead	3.03	All	All	All

cpe:2.3:a:jhead_project:jhead:3.03:*:*:*:*:*:*:*:

cpe:2.3:a:jhead_project:jhead:3.03:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→