CVE-2016-9581

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-9581
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-01 14:29:00 UTC
Updated	2023-02-12 23:27:00 UTC
Description	An infinite loop vulnerability in tiftoimage that results in heap buffer overflow in convert_32s_C1P1 was found in openjpeg 2

Risk And Classification

Problem Types: CWE-122 | CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Uclouvain	Openjpeg	2.1.2	All	All	All
Application	Uclouvain	Openjpeg	2.1.2	All	All	All

References

Reference
OpenJPEG: Multiple vulnerabilities (GLSA 201710-26) — Gentoo security
Out-of-Bounds Write issue can occur in function convert_32s_C1P1 (openjpeg-2.1.2/src/bin/jp2/convert.c:153) · Issue #872 · uclouvain/openjp
OpenJPEG Multiple Remote Heap Based Buffer Overflow Vulnerabilities
1405135 – (CVE-2016-9581) CVE-2016-9581 openjpeg2: Infinite loop in tiftoimage resulting into heap buffer overflow in convert_32s_C1P1
These changes repair bugs of #871 and #872 · szukw000/openjpeg@cadff5f · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500464 Alpine Linux Security Update for openjpeg

504221 Alpine Linux Security Update for openjpeg

710394 Gentoo Linux OpenJPEG Multiple Vulnerabilities (GLSA 201710-26)