National Critical Information Infrastructure Protection Centre

CVE Report

CV Scoring Scale : 3-10 01-15 Mar 2018 Vol. 05 No.05

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference /Patch	NCIIPC ID
Application					
Cimg					
Cimg					
Overflow	02-03-2018	6.8	An issue was discovered in CImg v.220. A heap-based buffer over-read in load_bmp in CImg.h occurs when loading a crafted bmp image, a different vulnerability than CVE-2018-7588. This is in a "32 bits colors" case, aka case 32. **CVE ID : CVE-2018-7641**	https://github.com/dtschump/CImg/issues/185	A-CIM-CIMG-160318/1
Overflow	02-03-2018	6.8	An issue was discovered in CImg v.220. A heap-based buffer over-read in load_bmp in CImg.h occurs when loading a crafted bmp image, a different vulnerability than CVE-2018-7588. This is in a Monochrome case, aka case 1. **CVE ID : CVE-2018-7640**	https://github.com/dtschump/CImg/issues/185	A-CIM-CIMG-160318/2
Overflow	02-03-2018	6.8	An issue was discovered in CImg v.220. A heap-based buffer over-read in load_bmp in CImg.h occurs when loading a crafted bmp image, a different vulnerability than CVE-2018-7588. This is in a "16 bits colors" case, aka case 16. **CVE ID : CVE-2018-7639**	https://github.com/dtschump/CImg/issues/185	A-CIM-CIMG-160318/3
Overflow	02-03-2018	6.8	An issue was discovered in CImg v.220. A heap-based buffer over-read in load_bmp in CImg.h occurs when loading a crafted bmp image, a different vulnerability than CVE-2018-7588. This is in a "256 colors" case, aka case 8. **CVE ID : CVE-2018-7638**	https://github.com/dtschump/CImg/issues/185	A-CIM-CIMG-160318/4
Overflow	02-03-2018	6.8	An issue was discovered in CImg v.220. A heap-based buffer over-read in load_bmp in CImg.h occurs when loading a crafted bmp image, a different vulnerability than CVE-2018-7588. This is in a "16 colors" case, aka case 4. **CVE ID : CVE-2018-7637**	https://github.com/dtschump/CImg/issues/185	A-CIM-CIMG-160318/5

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;