



Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHPC ID
			allows remote attackers to cause a denial of service (ImportIndexQuantumType invalid write and application crash) or possibly have unspecified other impact via a malformed WPG image. CVE ID : CVE-2017-16545	phicsmagick/code/rev/e8086faa52d0	
DoS	06-11-2017	6.8	The DrawImage function in magick/render.c in GraphicsMagick 1.3.26 does not properly look for pop keywords that are associated with push keywords, which allows remote attackers to cause a denial of service (negative strncpy and application crash) or possibly have unspecified other impact via a crafted file. CVE ID : CVE-2017-16547	https://sourceforge.net/p/graphicsmagick/bugs/517/	A-GRA-GRAPH-161117/4

Imagemagick

Imagemagick

DoS Overflow	05-11-2017	6.8	<p>The ReadWPGImage function in coders/wpg.c in ImageMagick 7.0.7-9 does not properly validate the colormap index in a WPG palette, which allows remote attackers to cause a denial of service (use of uninitialized data or invalid memory allocation) or possibly have unspecified other impact via a malformed WPG file.</p> <p>CVE ID : CVE-2017-16546</p>	https://github.com/ImageMagick/ImageMagick/issues/851	A-IMA-IMAGE-161117/5
--------------	------------	-----	---	---	----------------------

Mahara

Mahara

Gain Information	03-11-2017	3.5	Mahara 15.04 before 15.04.13 and 16.04 before 16.04.7 and 16.10 before 16.10.4 and 17.04 before 17.04.2 are vulnerable to recording plain text passwords in the event_log table during the	https://bugs.l aunchp ad.net/ mahar a/+bug	A-MAH- MAHAR- 161117/6
------------------	------------	-----	--	---	------------------------------

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;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user creation process if full event logging was turned on. CVE ID : CVE-2017-1000157	/1692749	
XSS	03-11-2017	3.5	Mahara 1.10 before 1.10.9 and 15.04 before 15.04.6 and 15.10 before 15.10.2 are vulnerable to XSS due to window.opener (target="_blank" and window.open()) CVE ID : CVE-2017-1000149	https://bugs.l aunchp ad.net/ mahar a/+bug /1558 361	A-MAH- MAHAR- 161117/7
XSS	03-11-2017	3.5	Mahara 1.9 before 1.9.7 and 1.10 before 1.10.5 and 15.04 before 15.04.2 are vulnerable to the arbitrary execution of Javascript in the browser of a logged-in user because the title of the portfolio page was not being properly escaped in the AJAX script that updates the Add/remove watchlist link on artefact detail pages. CVE ID : CVE-2017-1000146	https://bugs.l aunchp ad.net/ mahar a/+bug /1472 439	A-MAH- MAHAR- 161117/8
XSS	03-11-2017	3.5	Mahara 1.9 before 1.9.6 and 1.10 before 1.10.4 and 15.04 before 15.04.1 are vulnerable to a site admin or institution admin being able to place HTML and Javascript into an institution display name, which will be displayed to other users unescaped on some Mahara system pages. CVE ID : CVE-2017-1000144	https://bugs.l aunchp ad.net/ mahar a/+bug /1447 377	A-MAH- MAHAR- 161117/9
Execute Code XSS	03-11-2017	3.5	Mahara 1.8 before 1.8.7 and 1.9 before 1.9.5 and 1.10 before 1.10.3 and 15.04 before 15.04.0 are vulnerable to a maliciously created .xml file that can have its code executed when user tries to download the file. CVE ID : CVE-2017-1000140	https://bugs.l aunchp ad.net/ mahar a/+bug /1404 117	A-MAH- MAHAR- 161117/ 10

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;							

[illegible]

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			anonymous comments. CVE ID : CVE-2017-1000145	368	
Gain Information	03-11-2017	4	Mahara 1.8 before 1.8.7 and 1.9 before 1.9.5 and 1.10 before 1.10.3 and 15.04 before 15.04.0 are vulnerable to users receiving watchlist notifications about pages they do not have access to anymore. CVE ID : CVE-2017-1000143	https://bugs.l aunchp ad.net/ mahar a/+bug /1429 647	A-MAH- MAHAR- 161117/ 16
NA	03-11-2017	4	Mahara 1.8 before 1.8.7 and 1.9 before 1.9.5 and 1.10 before 1.10.3 and 15.04 before 15.04.0 are vulnerable as logged-in users can stay logged in after the institution they belong to is suspended. CVE ID : CVE-2017-1000135	https:// /bugs.l aunchp ad.net/ mahar a/+bug /1348 024	A-MAH- MAHAR- 161117/ 17
NA	03-11-2017	4	Mahara 15.04 before 15.04.8 and 15.10 before 15.10.4 and 16.04 before 16.04.2 are vulnerable to users staying logged in to their Mahara account even when they have been logged out of Moodle (when using MNet) as Mahara did not properly implement one of the MNet SSO API functions. CVE ID : CVE-2017-1000131	https:// /bugs.l aunchp ad.net/ mahar a/+bug /1084 336	A-MAH- MAHAR- 161117/ 18
NA	03-11-2017	4.3	Mahara 1.8 before 1.8.6 and 1.9 before 1.9.4 and 1.10 before 1.10.1 and 15.04 before 15.04.0 are vulnerable to old sessions not being invalidated after a password change. CVE ID : CVE-2017-1000136	https:// /bugs.l aunchp ad.net/ mahar a/+bug /1363 873	A-MAH- MAHAR- 161117/ 19
Gain Information	03-11-2017	5	Mahara 15.04 before 15.04.9 and 15.10 before 15.10.5 and 16.04 before 16.04.3 are vulnerable to passwords or other sensitive information being passed by unusual parameters to end up in	https:// /bugs.l aunchp ad.net/ mahar a/+bug	A-MAH- MAHAR- 161117/ 20

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;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an error log. CVE ID : CVE-2017-1000151	/1570 221	
Gain Information	03-11-2017	5	Mahara 15.04 before 15.04.8 and 15.10 before 15.10.4 and 16.04 before 16.04.2 are vulnerable to a user - in some circumstances causing another user's artefacts to be included in a Leap2a export of their own pages. CVE ID : CVE-2017-1000133	https:// bugs.l aunchp ad.net/ mahar a/+bug /1234 615	A-MAH- MAHAR- 161117/ 21
NA	03-11-2017	5.5	Mahara 15.04 before 15.04.9 and 15.10 before 15.10.5 and 16.04 before 16.04.3 are vulnerable to a group's configuration page being editable by any group member even when they didn't have the admin role. CVE ID : CVE-2017-1000156	https:// bugs.l aunchp ad.net/ mahar a/+bug /1609 200	A-MAH- MAHAR- 161117/ 22
NA	03-11-2017	5.5	Mahara 1.8 before 1.8.7 and 1.9 before 1.9.5 and 1.10 before 1.10.3 and 15.04 before 15.04.0 are vulnerable to users being able to delete their submitted page through URL manipulation. CVE ID : CVE-2017-1000142	https:// bugs.l aunchp ad.net/ mahar a/+bug /1425 306	A-MAH- MAHAR- 161117/ 23
CSRF	03-11-2017	6	Mahara 1.9 before 1.9.8 and 1.10 before 1.10.6 and 15.04 before 15.04.3 are vulnerable to perform a cross-site request forgery (CSRF) attack on the uploader contained in Mahara's filebrowser widget. This could allow an attacker to trick a Mahara user into unknowingly uploading malicious files into their Mahara account. CVE ID : CVE-2017-1000147	https:// bugs.l aunchp ad.net/ mahar a/+bug /1480 329	A-MAH- MAHAR- 161117/ 24
NA	03-11-2017	6	Mahara 1.8 before 1.8.7 and 1.9 before 1.9.5 and 1.10 before 1.10.3 and 15.04 before 15.04.0 are vulnerable to server-side	https:// bugs.l aunchp ad.net/ ad.net/	A-MAH- MAHAR- 161117/ 25

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request forgery attacks as not all processes of curl redirects are checked against a white or black list. Employing SafeCurl will prevent issues. CVE ID : CVE-2017-1000139	mahara/+bug/1397736	
NA	03-11-2017	6.5	Mahara 15.04 before 15.04.7 and 15.10 before 15.10.3 are vulnerable to prevent session IDs from being regenerated on login or logout. This makes users of the site more vulnerable to session fixation attacks. CVE ID : CVE-2017-1000150	https://bugs.launchpad.net/mahara/+bug/1567784	A-MAH-MAHAR-161117/26
Execute Code	03-11-2017	6.5	Mahara 15.04 before 15.04.8 and 15.10 before 15.10.4 and 16.04 before 16.04.2 are vulnerable to PHP code execution as Mahara would pass portions of the XML through the PHP "unserialize()" function when importing a skin from an XML file. CVE ID : CVE-2017-1000148	https://bugs.launchpad.net/mahara/+bug/1508684	A-MAH-MAHAR-161117/27
NA	03-11-2017	6.5	Mahara 1.8 before 1.8.6 and 1.9 before 1.9.4 and 1.10 before 1.10.1 and 15.04 before 15.04.0 are vulnerable because group members can lose access to the group files they uploaded if another group member changes the access permissions on them. CVE ID : CVE-2017-1000134	https://bugs.launchpad.net/mahara/+bug/1267686	A-MAH-MAHAR-161117/28
NA	03-11-2017	7.5	Mahara 15.04 before 15.04.8 and 15.10 before 15.10.4 and 16.04 before 16.04.2 are vulnerable to some authentication methods, which do not use Mahara's built-in login form, still allowing users to log in even if their institution was expired or suspended. CVE ID : CVE-2017-1000154	https://bugs.launchpad.net/mahara/+bug/1580399	A-MAH-MAHAR-161117/29
NA	03-11-2017	7.5	Mahara 15.04 before 15.04.10	https://	A-MAH-

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;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			and 15.10 before 15.10.6 and 16.04 before 16.04.4 are vulnerable to incorrect access control after the password reset link is sent via email and then user changes default email, Mahara fails to invalidate old link. Consequently the link in email can be used to gain access to the user's account. CVE ID : CVE-2017-1000153	/bugs.l aunchp ad.net/ mahar a/+bug /1577 251	MAHAR- 161117/ 30
NA	03-11-2017	7.5	Mahara 15.04 before 15.04.7 and 15.10 before 15.10.3 running PHP 5.3 are vulnerable to one user being logged in as another user on a separate computer as the same session ID is served. This situation can occur when a user takes an action that forces another user to be logged out of Mahara, such as an admin changing another user's account settings. CVE ID : CVE-2017-1000152	https:/ /bugs.l aunchp ad.net/ mahar a/+bug /1570 744	A-MAH- MAHAR- 161117/ 31
Radare					
Radare2					
NA	01-11-2017	4.3	In radare 2.0.1, a pointer wraparound vulnerability exists in store_versioninfo_gnu_verdef() in libr/bin/format/elf/elf.c. CVE ID : CVE-2017-16359	https:/ /githu b.com/ radare /radar e2/issu es/876 4	A-RAD- RADAR- 161117/ 32
NA	01-11-2017	6.8	In radare 2.0.1, an out-of-bounds read vulnerability exists in string_scan_range() in libr/bin/bin.c when doing a string search. CVE ID : CVE-2017-16358	https:/ /githu b.com/ radare /radar e2/issu es/874 8	A-RAD- RADAR- 161117/ 33

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;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHPC ID
Overflow; Memory Corruption	01-11-2017	6.8	In radare 2.0.1, a memory corruption vulnerability exists in store_versioninfo_gnu_verdef() and store_versioninfo_gnu_verneed() in libr/bin/format/elf/elf.c, as demonstrated by an invalid free. This error is due to improper sh_size validation when allocating memory. CVE ID : CVE-2017-16357	https://github.com/radare/radare2/issues/8742	A-RAD-RADAR-161117/34

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;							