



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

CVE	CVE-2015-3178
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-01 19:59:00 UTC
Updated	2020-12-01 14:54:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the external_format_text function in lib/externallib.php in Moodle through 2.5.9, 2.6.0, 2.7.0, 2.8.0, 2.9.0, 2.9.1, 2.9.2, 2.9.3, 2.9.4, 2.9.5, 2.9.6, 2.9.7, 2.9.8, 2.9.9, 2.9.10, 2.9.11, 2.9.12, 2.9.13, 2.9.14, 2.9.15, 2.9.16, 2.9.17, 2.9.18, 2.9.19, 2.9.20, 2.9.21, 2.9.22, 2.9.23, 2.9.24, 2.9.25, 2.9.26, 2.9.27, 2.9.28, 2.9.29, 2.9.30, 2.9.31, 2.9.32, 2.9.33, 2.9.34, 2.9.35, 2.9.36, 2.9.37, 2.9.38, 2.9.39, 2.9.40, 2.9.41, 2.9.42, 2.9.43, 2.9.44, 2.9.45, 2.9.46, 2.9.47, 2.9.48, 2.9.49, 2.9.50, 2.9.51, 2.9.52, 2.9.53, 2.9.54, 2.9.55, 2.9.56, 2.9.57, 2.9.58, 2.9.59, 2.9.60, 2.9.61, 2.9.62, 2.9.63, 2.9.64, 2.9.65, 2.9.66, 2.9.67, 2.9.68, 2.9.69, 2.9.70, 2.9.71, 2.9.72, 2.9.73, 2.9.74, 2.9.75, 2.9.76, 2.9.77, 2.9.78, 2.9.79, 2.9.80, 2.9.81, 2.9.82, 2.9.83, 2.9.84, 2.9.85, 2.9.86, 2.9.87, 2.9.88, 2.9.89, 2.9.90, 2.9.91, 2.9.92, 2.9.93, 2.9.94, 2.9.95, 2.9.96, 2.9.97, 2.9.98, 2.9.99, 2.9.100, 2.9.101, 2.9.102, 2.9.103, 2.9.104, 2.9.105, 2.9.106, 2.9.107, 2.9.108, 2.9.109, 2.9.110, 2.9.111, 2.9.112, 2.9.113, 2.9.114, 2.9.115, 2.9.116, 2.9.117, 2.9.118, 2.9.119, 2.9.120, 2.9.121, 2.9.122, 2.9.123, 2.9.124, 2.9.125, 2.9.126, 2.9.127, 2.9.128, 2.9.129, 2.9.130, 2.9.131, 2.9.132, 2.9.133, 2.9.134, 2.9.135, 2.9.136, 2.9.137, 2.9.138, 2.9.139, 2.9.140, 2.9.141, 2.9.142, 2.9.143, 2.9.144, 2.9.145, 2.9.146, 2.9.147, 2.9.148, 2.9.149, 2.9.150, 2.9.151, 2.9.152, 2.9.153, 2.9.154, 2.9.155, 2.9.156, 2.9.157, 2.9.158, 2.9.159, 2.9.160, 2.9.161, 2.9.162, 2.9.163, 2.9.164, 2.9.165, 2.9.166, 2.9.167, 2.9.168, 2.9.169, 2.9.170, 2.9.171, 2.9.172, 2.9.173, 2.9.174, 2.9.175, 2.9.176, 2.9.177, 2.9.178, 2.9.179, 2.9.180, 2.9.181, 2.9.182, 2.9.183, 2.9.184, 2.9.185, 2.9.186, 2.9.187, 2.9.188, 2.9.189, 2.9.190, 2.9.191, 2.9.192, 2.9.193, 2.9.194, 2.9.195, 2.9.196, 2.9.197, 2.9.198, 2.9.199, 2.9.200, 2.9.201, 2.9.202, 2.9.203, 2.9.204, 2.9.205, 2.9.206, 2.9.207, 2.9.208, 2.9.209, 2.9.210, 2.9.211, 2.9.212, 2.9.213, 2.9.214, 2.9.215, 2.9.216, 2.9.217, 2.9.218, 2.9.219, 2.9.220, 2.9.221, 2.9.222, 2.9.223, 2.9.224, 2.9.225, 2.9.226, 2.9.227, 2.9.228, 2.9.229, 2.9.230, 2.9.231, 2.9.232, 2.9.233, 2.9.234, 2.9.235, 2.9.236, 2.9.237, 2.9.238, 2.9.239, 2.9.240, 2.9.241, 2.9.242, 2.9.243, 2.9.244, 2.9.245, 2.9.246, 2.9.247, 2.9.248, 2.9.249, 2.9.250, 2.9.251, 2.9.252, 2.9.253, 2.9.254, 2.9.255, 2.9.256, 2.9.257, 2.9.258, 2.9.259, 2.9.260, 2.9.261, 2.9.262, 2.9.263, 2.9.264, 2.9.265, 2.9.266, 2.9.267, 2.9.268, 2.9.269, 2.9.270, 2.9.271, 2.9.272, 2.9.273, 2.9.274, 2.9.275, 2.9.276, 2.9.277, 2.9.278, 2.9.279, 2.9.280, 2.9.281, 2.9.282, 2.9.283, 2.9.284, 2.9.285, 2.9.286, 2.9.287, 2.9.288, 2.9.289, 2.9.290, 2.9.291, 2.9.292, 2.9.293, 2.9.294, 2.9.295, 2.9.296, 2.9.297, 2.9.298, 2.9.299, 2.9.300, 2.9.301, 2.9.302, 2.9.303, 2.9.304, 2.9.305, 2.9.306, 2.9.307, 2.9.308, 2.9.309, 2.9.310, 2.9.311, 2.9.312, 2.9.313, 2.9.314, 2.9.315, 2.9.316, 2.9.317, 2.9.318, 2.9.319, 2.9.320, 2.9.321, 2.9.322, 2.9.323, 2.9.324, 2.9.325, 2.9.326, 2.9.327, 2.9.328, 2.9.329, 2.9.330, 2.9.331, 2.9.332, 2.9.333, 2.9.334, 2.9.335, 2.9.336, 2.9.337, 2.9.338, 2.9.339, 2.9.340, 2.9.341, 2.9.342, 2.9.343, 2.9.344, 2.9.345, 2.9.346, 2.9.347, 2.9.348, 2.9.349, 2.9.350, 2.9.351, 2.9.352, 2.9.353, 2.9.354, 2.9.355, 2.9.356, 2.9.357, 2.9.358, 2.9.359, 2.9.360, 2.9.361, 2.9.362, 2.9.363, 2.9.364, 2.9.365, 2.9.366, 2.9.367, 2.9.368, 2.9.369, 2.9.370, 2.9.371, 2.9.372, 2.9.373, 2.9.374, 2.9.375, 2.9.376, 2.9.377, 2.9.378, 2.9.379, 2.9.380, 2.9.381, 2.9.382, 2.9.383, 2.9.384, 2.9.385, 2.9.386, 2.9.387, 2.9.388, 2.9.389, 2.9.390, 2.9.391, 2.9.392, 2.9.393, 2.9.394, 2.9.395, 2.9.396, 2.9.397, 2.9.398, 2.9.399, 2.9.400, 2.9.401, 2.9.402, 2.9.403, 2.9.404, 2.9.405, 2.9.406, 2.9.407, 2.9.408, 2.9.409, 2.9.410, 2.9.411, 2.9.412, 2.9.413, 2.9.414, 2.9.415, 2.9.416, 2.9.417, 2.9.418, 2.9.419, 2.9.420, 2.9.421, 2.9.422, 2.9.423, 2.9.424, 2.9.425, 2.9.426, 2.9.427, 2.9.428, 2.9.429, 2.9.430, 2.9.431, 2.9.432, 2.9.433, 2.9.434, 2.9.435, 2.9.436, 2.9.437, 2.9.438, 2.9.

Problem Types: CWE-79

Type	Vendor	Product	Version	Update	Edition	Language
Application	Moodle	Moodle	2.5.0	All	All	All
Application	Moodle	Moodle	2.5.1	All	All	All
Application	Moodle	Moodle	2.5.2	All	All	All
Application	Moodle	Moodle	2.5.3	All	All	All
Application	Moodle	Moodle	2.5.4	All	All	All
Application	Moodle	Moodle	2.5.5	All	All	All
Application	Moodle	Moodle	2.5.6	All	All	All
Application	Moodle	Moodle	2.5.7	All	All	All
Application	Moodle	Moodle	2.5.8	All	All	All
Application	Moodle	Moodle	2.6.0	All	All	All
Application	Moodle	Moodle	2.6.1	All	All	All
Application	Moodle	Moodle	2.6.10	All	All	All
Application	Moodle	Moodle	2.6.2	All	All	All
Application	Moodle	Moodle	2.6.3	All	All	All
Application	Moodle	Moodle	2.6.4	All	All	All
Application	Moodle	Moodle	2.6.5	All	All	All
Application	Moodle	Moodle	2.6.6	All	All	All

Application	Moodle	Moodle	2.6.7	All	All	All
Application	Moodle	Moodle	2.6.8	All	All	All
Application	Moodle	Moodle	2.6.9	All	All	All
Application	Moodle	Moodle	2.7.0	All	All	All
Application	Moodle	Moodle	2.7.1	All	All	All
Application	Moodle	Moodle	2.7.2	All	All	All
Application	Moodle	Moodle	2.7.3	All	All	All
Application	Moodle	Moodle	2.7.4	All	All	All
Application	Moodle	Moodle	2.7.5	All	All	All
Application	Moodle	Moodle	2.7.6	All	All	All
Application	Moodle	Moodle	2.7.7	All	All	All
Application	Moodle	Moodle	2.8.0	All	All	All
Application	Moodle	Moodle	2.8.1	All	All	All
Application	Moodle	Moodle	2.8.2	All	All	All
Application	Moodle	Moodle	2.8.3	All	All	All
Application	Moodle	Moodle	2.8.4	All	All	All
Application	Moodle	Moodle	2.8.5	All	All	All
Application	Moodle	Moodle	2.5.0	All	All	All
Application	Moodle	Moodle	2.5.1	All	All	All
Application	Moodle	Moodle	2.5.2	All	All	All
Application	Moodle	Moodle	2.5.3	All	All	All
Application	Moodle	Moodle	2.5.4	All	All	All
Application	Moodle	Moodle	2.5.5	All	All	All
Application	Moodle	Moodle	2.5.6	All	All	All
Application	Moodle	Moodle	2.5.7	All	All	All
Application	Moodle	Moodle	2.5.8	All	All	All
Application	Moodle	Moodle	2.6.0	All	All	All
Application	Moodle	Moodle	2.6.1	All	All	All
Application	Moodle	Moodle	2.6.10	All	All	All
Application	Moodle	Moodle	2.6.2	All	All	All
Application	Moodle	Moodle	2.6.3	All	All	All
Application	Moodle	Moodle	2.6.4	All	All	All
Application	Moodle	Moodle	2.6.5	All	All	All
Application	Moodle	Moodle	2.6.6	All	All	All
Application	Moodle	Moodle	2.6.7	All	All	All

Application	Moodle	Moodle	2.6.8	All	All	All
Application	Moodle	Moodle	2.6.9	All	All	All
Application	Moodle	Moodle	2.7.0	All	All	All
Application	Moodle	Moodle	2.7.1	All	All	All
Application	Moodle	Moodle	2.7.2	All	All	All
Application	Moodle	Moodle	2.7.3	All	All	All
Application	Moodle	Moodle	2.7.4	All	All	All
Application	Moodle	Moodle	2.7.5	All	All	All
Application	Moodle	Moodle	2.7.6	All	All	All
Application	Moodle	Moodle	2.7.7	All	All	All
Application	Moodle	Moodle	2.8.0	All	All	All
Application	Moodle	Moodle	2.8.1	All	All	All
Application	Moodle	Moodle	2.8.2	All	All	All
Application	Moodle	Moodle	2.8.3	All	All	All
Application	Moodle	Moodle	2.8.4	All	All	All
Application	Moodle	Moodle	2.8.5	All	All	All
Application	Moodle	Moodle	All	All	All	All

References

Reference

Moodle CVE-2015-3178 Cross Site Scripting Vulnerability

Moodle.org: MSA-15-0022: Potential XSS risk when returning text entered by student from Web Services

oss-security - Moodle security advisories [vs]

Moodle Multiple Flaws Let Remote Users Conduct Cross-Site Scripting Attacks, Obtain Potentially Sensitive Information, and Bypass Security

Official Moodle git projects - moodle.git/search

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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