

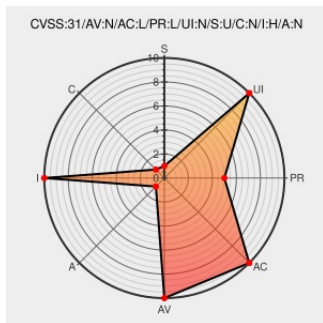


CVE-2019-18212

Published on: 10/23/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:06 PM UTC

CVE-2019-18212

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Wild Web Developer](#) from [Eclipse](#) contain the following vulnerability:

XMLLanguageService.java in XML Language Server (aka lsp4xml) before 0.9.1, as used in Red Hat XML Language Support (aka vscode-xml) before 0.9.1 for Visual Studio and other products, allows a remote attacker to write to arbitrary files via Directory Traversal.

CVE-2019-18212 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Don't open that XML: XXE to RCE in XML plugins for VS Code, Eclipse, Theia, ... - Shielder	Exploit Third Party Advisory www.shielder.it text/html	MISC www.shielder.it/blog/dont-open-that-xml-xxe-to-rce-in-xml-plugins-for-vs-code-eclipse-theia/

lemminx/CHANGELOG.md at master · eclipse/lemminx · GitHub	Release Notes Third Party Advisory github.com text/html	 CONFIRM github.com/angelozerr/lsp4xml/blob/master/CHANGELOG.md#others
Reject download of resource which are not in the cache folder by angelozerr · Pull Request #567 · eclipse/lemminx · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/angelozerr/lsp4xml/pull/567
GitHub - angelozerr/lsp4xml: XML Language Server	Product github.com text/html	 MISC github.com/angelozerr/lsp4xml/
XML - Visual Studio Marketplace	Third Party Advisory marketplace.visualstudio.com text/html	 MISC marketplace.visualstudio.com/items?itemName=redhat.vscode-xml
GitHub - redhat-developer/vscode-xml: Editing XML in Visual Studio Code made easy	Patch Third Party Advisory github.com text/html	 MISC github.com/redhat-developer/vscode-xml/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eclipse	Wild Web Developer	-	All	All	All
Application	Eclipse	Wild Web Developer	-	All	All	All
Application	Theia Xml Extension Project	Theia Xml Extension	-	All	All	All
Application	Theia Xml Extension Project	Theia Xml Extension	-	All	All	All
Application	Xml Language Server Project	Xml Server Project	All	All	All	All
Application	Xml Language Server Project	Xml Server Project	All	All	All	All

cpe:2.3:a:eclipse:wild_web_developer:-:*****:

cpe:2.3:a:eclipse:wild_web_developer:-:*****:

cpe:2.3:a:theia_xml_extension_project:theia_xml_extension:-:*****:

cpe:2.3:a:theia_xml_extension_project:theia_xml_extension:-:*****:

cpe:2.3:a:xml_language_server_project:xml_server_project:*****:

cpe:2.3:a:xml_language_server_project:xml_server_project:*****:

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)