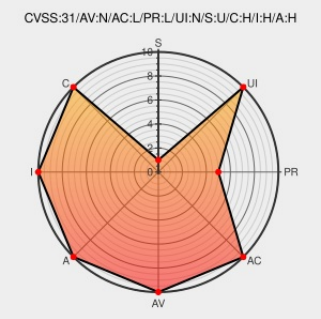
CVE-2019-18213

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

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-18213

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wild Web Developer from Eclipse contain the following vulnerability:

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 XXE via a crafted XML document, with resultant SSRF (as well as SMB connection initiation that can lead to NetNTLM challenge/response capture for password cracking). This occurs in extensions/contentmodel/participants/diagnostics/LSPXMLParserConfiguration.java.

CVE-2019-18213 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

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

Theia, ... - Shielder	www.shielder.it text/html	
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
Add disallowDocTypeDecl & resolveExternalEntities validation settings by angelozerr · Pull Request #566 · eclipse/lemminx · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/angelozerr/lsp4xml/pull/566
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/

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

← Previous ID

Next ID→