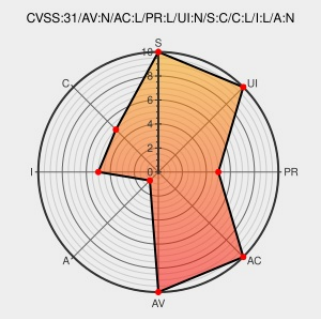
CVE-2021-21266

Published on: 02/01/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:57 PM UTC

CVE-2021-21266 - advisory for GHSA-r2hc-pmr7-4c9r

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



Certain versions of Openhab from Openhab contain the following vulnerability:

openHAB is a vendor and technology agnostic open source automation software for your home. In openHAB before versions 2.5.12 and 3.0.1 the XML external entity (XXE) attack allows attackers in the same network as the openHAB instance to retrieve internal information like the content of files from the file system. Responses to SSDP requests can be especially malicious. All add-ons that use SAX or JAXB parsing of externally received XML are potentially subject to this kind of attack. In openHAB, the following add-ons are potentially impacted: AvmFritz, BoseSoundtouch, DenonMarantz, DLinkSmarthome, Enigma2, FmiWeather, FSInternetRadio, Gce, Homematic, HPPrinter, IHC, Insteon, Onkyo, Roku, SamsungTV, Sonos, Roku, Tellstick, TR064, UPnPControl, Vitotronic, Wemo, YamahaReceiver and XPath Tranformation. The vulnerabilities have been fixed in versions 2.5.12 and 3.0.1 by a more strict configuration of the used XML parser.

CVE-2021-21266 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **openhab** - **openhab-addons** version **< 2.5.12**

Affected Vendor/Software: **openhab** - **openhab-addons** version **= 3.0.0**

CVSS3 Score: 5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication

Vector	Complexity	
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
XXE vulnerabilities in multiple add-ons · Advisory · openhab/openhab-addons · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/openhab/openhab-addons/security/advisories/GHSA-r2hc-pmr7-4c9r
Fix XXE vulnerabilities in multiple add-ons · openhab/openhab-addons@81935b0 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/openhab/openhab-addons/commit/81935b0ab126e6d9aebd2f6c3fc67d82bb7e8b86
Configure your Java XML-parsers to prevent XXE - DEV Community ????????????????	Third Party Advisory dev.to text/html	MISC dev.to/brianverm/configure-your-java-xml-parsers-to-prevent-xxe-213c
XML External Entity (XXE) Pitfalls With JAXB	Technical Description Third Party Advisory www.contrastsecurity.com application/octet-stream	MISC www.contrastsecurity.com/security-influencers/xml-xxe-pitfalls-with-jaxb

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openhab	Openhab	All	All	All	All
Application	Openhab	Openhab	3.0.0	All	All	All
Application	Openhab	Openhab	All	All	All	All
Application	Openhab	Openhab	3.0.0	All	All	All

cpe:2.3:a:openhab:openhab:*:*:*:*:*:*:*:*:

cpe:2.3:a:openhab:openhab:3.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:openhab:openhab:*:*:*:*:*:*:*:*:

cpe:2.3:a:openhab:openhab:3.0.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→