[CVE-2020-11991] Apache Cocoon security vulnerability

Posted to users@cocoon.apache.org (list.html?users@cocoon.apache.org)

Cédric Damioli - Friday, September 11, 2020 5:39:23 AM EDT

[CVE-2020-11991] Apache Cocoon security vulnerability

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: Apache Cocoon up to 2.1.12

Description: When using the StreamGenerator, the code parse a
user-provided XML.

A specially crafted XML, including external system entities, could be
used to access any file on the server system.

Mitigation:

The StreamGenerator now ignores external entities. 2.1.x users should
upgrade to 2.1.13

Example:

With the following input :

<!--?xml version="1.0" ?--> <!DOCTYPE replace [<!ENTITY ent SYSTEM
"file:///etc/shadow">]> <userInfo> <firstName>John</firstName>
<lastName>&ent;</lastName> </userInfo> an attacker got the content of
/etc/shadow

Credit: This issue was discovered by Nassim Asrir.

Regards,

--
Cédric Damioli

gelo1234 - Friday, September 11, 2020 6:12:02 AM EDT

Hello Cedric,

Are external entities blocked also in XSLT?

Greetings,
Greg

pt., 11 wrz 2020 o 11:39 Cédric Damioli <cd...@apache.org> napisał(a):

Cédric Damioli - Friday, September 11, 2020 3:46:23 PM EDT

Hi,

Entities resolution is managed by features of the SAX Parser, before any
transformation.

Cédric

Le 11/09/2020 à 12:12, gelo1234 a écrit :

--
Cédric Damioli
CMS - Java - Open Source
www.ametys.org