Analysis of the Sonatype Security Scan of Icefaces 4.3

This is an analysis of the results of the Sonatype Security Scan of Icefaces 4.3 provided to Icesoft in the file ICEfaces-EE-4.3.0.GA_P04-bin.pdf.

This analysis is only of the level 8 vulnerabilities, which are the ones the customer is more concerned about. Although, the report does not state it explicitly, we assume that level 8 vulnerabilities correspond to those which have a CVSS score of 8.8 and 7.5.

To summarize this analysis, none of the vulnerabilities reported have to do with our Icefaces code. All vulnerabilities reported are in external libraries that may or may not be used by Icefaces applications at runtime. In some cases, a newer version of a library (that does not contain the vulnerability) could be used, but this would require testing first to certify that the newer version works well with Icefaces. In most cases, as long as an Icefaces application is not using those libraries in other ways than in the one originally intended, it will not be exposed to these vulnerabilities.

List of Level 8 Vulnerabilities

- CVE-2015-0254
- CVE-2017-9096
- CVE-2017-12626
- CVE-2018-14371
- CVE-2021-26296
- CVE-2021-35515
- CVE-2021-35516
- CVE-2021-35517
- CVE-2021-36090
- sonatype-2017-0413
- sonatype-2018-0590

List of Occurrences by Item

- 4 in org.icefaces.samples : showcase : war : 4.3.0
- 4 in org.icefaces.samples : emporium : war : 4.3.0
- 4 in org.apache.commons : commons-compress : 1.20
- 3 in org.apache.myfaces.core : myfaces-bundle : 2.2.12 and org.apache.myfaces.core : myfaces-bundle : 2.3.6
- 1 in javax.servlet : jstl : 1.2
- 1 in rhino : js : 1.7R1

Description of Vulnerabilities

All this information is taken from the National Vulnerability Database (https://nvd.nist.gov/), from CVE (https://cve.mitre.org/) and from pages referenced by them.

- CVE-2015-0254 (org.icefaces.samples : showcase : war : 4.3.0, org.icefaces.samples : emporium : war : 4.3.0, javax.servlet : jstl : 1.2)

    - Apache Standard Taglibs before 1.2.3 allows remote attackers to execute arbitrary code or conduct external XML entity (XXE) attacks via a crafted XSLT extension in a (1) x:parse or (2) x:transform JSTL XML tag.
    - When an application uses x:parse or x:transform tags to process untrusted XML documents, a request may utilize external entity references to access resources on the host system or utilize XSLT extensions that may allow remote execution.
- CVE-2017-9096 (org.icefaces.samples : showcase : war : 4.3.0, org.icefaces.samples : emporium : war : 4.3.0)
    - The XML parsers in iText before 5.5.12 and 7.x before 7.0.3 do not disable external entities, which might allow remote attackers to conduct XML external entity (XXE) attacks via a crafted PDF.
    - The attack can be carried out by submitting a malicious PDF to an iText application that parses XML data.
      By providing a malicious XXE payloads inside the XML data that resides in the PDF, an attacker can for example extract files or forge requests on the server.
- CVE-2017-12626 (org.icefaces.samples : showcase : war : 4.3.0, org.icefaces.samples : emporium : war : 4.3.0)
    - Apache POI in versions prior to release 3.17 are vulnerable to Denial of Service Attacks: 1) Infinite Loops while parsing crafted WMF, EMF, MSG and macros (POI bugs 61338 and 61294), and 2) Out of Memory Exceptions while parsing crafted DOC, PPT and XLS (POI bugs 52372 and 61295).
    - Mitigation: Users with applications which accept content from external or untrusted sources are advised to upgrade to Apache POI 3.17 or newer.
- CVE-2018-14371 (org.icefaces.samples : showcase : war : 4.3.0, org.icefaces.samples : emporium : war : 4.3.0)
    - The getLocalePrefix function in ResourceManager.java in Eclipse Mojarra before 2.3.7 is affected by Directory Traversal via the loc parameter. A remote attacker can download configuration files or Java bytecodes from applications.s
- CVE-2021-26296 (org.apache.myfaces.core : myfaces-bundle : 2.2.12, org.apache.myfaces.core : myfaces-bundle : 2.3.6)
    - In the default configuration, Apache MyFaces Core versions 2.2.0 to 2.2.13, 2.3.0 to 2.3.7, 2.3-next-M1 to 2.3-next-M4, and 3.0.0-RC1 use cryptographically weak implicit and explicit cross-site request forgery (CSRF) tokens. Due to that limitation, it is possible (although difficult) for an attacker to calculate a future CSRF token value and to use that value to trick a user into executing unwanted actions on an application.
- CVE-2021-35515 (org.apache.commons : commons-compress : 1.20)
    - When reading a specially crafted 7Z archive, the construction of the list of codecs that decompress an entry can result in an infinite loop. This could be used to mount a denial of service attack against services that use Compress' sevenz package.
- CVE-2021-35516 (org.apache.commons : commons-compress : 1.20)
    - When reading a specially crafted 7Z archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' sevenz package.
- CVE-2021-35517 (org.apache.commons : commons-compress : 1.20)
    - When reading a specially crafted TAR archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small

inputs. This could be used to mount a denial of service attack against services that use Compress' tar package.

- CVE-2021-36090 (org.apache.commons : commons-compress : 1.20)
  - When reading a specially crafted ZIP archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' zip package.
- sonatype-2017-0413 (org.apache.myfaces.core : myfaces-bundle : 2.2.12)
  - No official information was found on this vulnerability.
  - The following information was found on https://blog.sonatype.com/top-5-tomcat-vulnerabilities
    - The vulnerability relies on modifying view state. For the demo, we have a simple app that tracks the name of a person to say hello to. It's your traditional hello world app. This exploit works by running the JexBoss exploit tool against the app. From the attacking server, we're able to create a shell into the server running the hello world app. And the attacker now has access to everything.
- sonatype-2018-0590 (rhino : js : 1.7R1)
  - No information was found on this vulnerability.

Observations

- CVE-2015-0254
  - If an Icefaces application does not use JSTL at all, there is no risk. If the application uses it there is still no risk as long as it does not use x:parse and x:transform to process untrusted XML documents provided by end users.
- CVE-2017-9096
  - In Icefaces, the iText library is only used to export data in the PDF format. If an Icefaces application does not need to export data in the PDF format, it does not require the iText library at all. So, it can be removed, which completely eliminates the risk. If the iText library is included in an Icefaces application, as long as it is not used for something other than its original purpose, especially as long as it is not used to process PDF files submitted by end users, then the risk is absent.
- CVE-2017-12626
  - As with CVE-2017-9096, the POI library is only used to export data in the XLS format. If an Icefaces application does not need to export data in the XLS format, it does not require the POI library at all. So, it can be removed, which completely eliminates the risk. If the POI library is included in an Icefaces application, as long as it is not used for something other than its original purpose, especially as long as it is not used to process WMF, EMF, MSG, DOC, PPT, and XLS files submitted by end users, then the risk is absent.
- CVE-2021-35515, CVE-2021-35516, CVE-2021-35517, and CVE-2021-36090
  - The commons-compress-1.20.jar library is a dependency of the POI library. If data exporting to the XLS format is not required by an Icefaces application, then this library is not necessary at runtime, and the risk is completely absent. If data exporting to the XLS format is required by an Icefaces application, then, as long as this library is not used for anything other than its original purpose, especially, if it is not used to read 7Z, ZIP, or TAR archives, then the reisk is absent.

- CVE-2018-14371
    - This vulnerability is reported in the Eclipse Mojarra library. The report states that versions before 2.3.7 are vulnerable. Icefaces is shipped with Eclipse Mojarra version 2.3.14. So, in theory, it is not vulnerable to this exploit. This has to be reviewed/confirmed.
- CVE-2021-26296, and sonatype-2017-0413
    - These vulnerabilities only apply to MyFaces. If MyFaces is not being used, then the risk is absent.
- sonatype-2018-0590
    - The rhino package is inside js-compiler.jar, which is not used at runtime. It is only used at compile time for compiling our Javascript code.