[2020-06-03] Change Log

Contents:

1. Improve Java parser to support 13 & 14 versions (also review v12)

There have been two updates on Java:

- Java 13 went GA on September 17, 2019
- Java 14 went GA on March 17, 2020

We have made language syntax changes for Java 13 and 14:

- Switch Expressions
- Text Blocks
- Pattern Matching for Instanceof
- Records

2. Improve C/C++ technology support

Our analysis engine now has support for the Tainting Propagation Algorithm and the Local Symbol Table, giving us better support for the detection of vulnerabilities.

We have also added 23 new rules and improved many of the existing ones for both C and C++:

1. Weak symmetric encryption algorithm (CWE:327, OWASP-M:2014:M4, SANS25:2011:19, OWASP:2017:A3, SANS25:2010:24, PCI-DSS:6.5.3, OWASP:2013:A6, WASC:04)
2. Weak cryptographic hash (CWE:327, OWASP:2017:A3, WASC:50, PCI-DSS:6.5.3)
3. Avoid unintended access to filesystem resources outside the chroot directory (CWE:243)
4. Unsafe chroot call (CWE:243, CERT-D:POS05)
5. Static database connection/session (CWE:567, PCI-DSS:6.5.6)
6. Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (OWASP:2017:A1, WASC:19, CWE:89, OWASP:2013:A1, SANS25:2010:2, SANS25:2011:1, PCI-DSS:6.5.1, CWETOP25:2019:6)
7. Improper control of resource identifiers ("Resource Injection")(CWE:99, OWASP:2017:A5, OWASP-M:2014:M8, WASC:20, PCI-DSS:6.5.1)
8. Do not load executables or libraries from untrusted sources (CWE:114, CWE:494, OWASP:2013:A4, WASC:20, SANS25:2010:20, SANS25:2011:14, PCI-DSS:6.5.8)
9. Avoid non-neutralized user-controlled input composed in a pathname to a resource (CWE:22, CWE:73, OWASP:2017:A5, OWASP:2013:A4, CERT-C:FIO01, WASC:33, PCI-DSS:6.5.8, CWETOP25:2019:10)
10. Improper neutralization of special elements in data query logic (NoSQL injection) (CWE:943, OWASP:2017:A1, WASC:19, OWASP-M:2014:M7, SANS25:2011:1, PCI-DSS:6.5.1)
11. Avoid non-neutralized user-controlled input in LDAP search filters (CWE:90, OWASP:2017:A1, WASC:29, PCI-DSS:6.5.1)
12. Weak cryptography, insufficient key length (CWE:326, OWASP:2017:A3, OWASP-M:2014:M6, PCI-DSS:6.5.3)
13. Insecure SSL configuration (CWE:296, CWE:297, CWE:298, CWE:299, OWASP-M:2014:M3, OWASP:2013:A6, WASC:04, PCI-DSS:6.5.4)
14. Standard pseudo-random number generators cannot withstand cryptographic attacks (CWE:330, CWE:338, CERT-C:MSC30, OWASP:2017:A3, OWASP-M:2014:M6, PCI-DSS:6.5.3)
15. Use of Hard-coded Credentials (CWE:798, OWASP:2017:A5, OWASP-M:2014:M2, SANS25:2011:7, WASC:01, PCI-DSS:6.5.3, CWETOP25:2019:19)
16. Use of hardcoded salt (CWE:760, OWASP:2013:A6, PCI-DSS:6.5.3)
17. Hardcoded cryptographic keys (CWE:321, OWASP:2017:A3, OWASP-M:2014:M6, PCI-DSS:6.3.1, WASC:13)
18. Prevent denial of service attack through malicious regular expression ('Regex Injection')(CWE:400,CWETOP25:2019:20)
19. Connection string polluted with untrusted input (CWE:99, OWASP:2013:A1, WASC:20, PCI-DSS:6.5.1)
20. Access Control - Anonymous LDAP Bind (CWE:285, OWASP:2017:A5, SANS25:2010:5, PCI-DSS:6.5.8)

21. Do not use deprecated or obsolete functions (CERT-C:MSC24)
22. Do not hardcode absolute paths (CWE:426,CWETOP25:2019:22)
23. XML entity injection (CWE:611, CWE:776, OWASP:2017:A4, WASC:43, WASC:44, PCI-DSS: 6.5.1, CWETOP25:2019:17)

3. New Java/JSP rules

We have added 3 new rules:

1. Spring CSRF unrestricted RequestMapping (CWE:352, WASC:9, SANS25:2010:4, OWASP: 2013:A8, SANS25:2011:12, PCI-DSS:6.5.1, CWETOP25:2019:9)
2. Improper Neutralization of Input leads to Reflected File Download (CWE:79, OWASP:2017:A1, OWASP:2013:A1, SANS25:2010:9, SANS25:2011:2, OWASP-M:2014:M7, CWETOP25:2019:2)
3. Specify a integrity attribute on the <script> and <link> elements

4. Django Framework Update

The Django framework has been updated to support up to version 3.0

5. AcuCOBOL Parser Update

The AcuCOBOL parser was updated with support for AcuCOBOL-GT 13.0 and the (few) extensions for Veryant isCOBOL

6. Auto-Disabling of Accounts

Now you can configure auto-disabling of user accounts due to inactivity: Account Policies

7. New tag for CWE 2019 Top 25 Most Dangerous Software Errors

See more: https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html

8. New API REST endpoints

GET /deliveries/last_analysis : retrieve the results of last delivery analysis

You can get all API REST endpoint and details at https://static.kiuwan.com/rest-api/kiuwan-rest-api.html

9. CQM v2.6.0

We have released a new version of CQM, our default analysis mode. Find instructions on how to compare this new model to the previous versions here: Comparing Models