Parasoft Support for CWE Top 25 + On the Cusp 2019 in C/C++test 2020.1

The following table shows how CWE Top 25 Most Dangerous Software Errors and Weaknesses On the Cusp 2019 (CWE Top 25 + On the Cusp 2019) maps to Parasoft's static analysis rules for C/C++.

ID	Kind	Name/description	Parasoft rule ID(s)
CWE-119	Top 25	Improper Restriction of Operations within the Bounds of a Memory Buffer	CWE-119-a, CWE-119-b, CWE-119-c, CWE-119-d, CWE-119-e, CWE-119-f, CWE-119-g, CWE-119-h, CWE-119-i, CWE-119-j
CWE-79	Top 25	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	N/A
CWE-20	Top 25	Improper Input Validation	CWE-20-a, CWE-20-b, CWE-20-c, CWE-20-d, CWE-20-e, CWE-20-f, CWE-20-g, CWE-20-h, CWE-20-i, CWE-20-j
CWE-200	Top 25	Information Exposure	CWE-200-a
CWE-125	Top 25	Out-of-bounds Read	CWE-125-a, CWE-125-b, CWE-125-c, CWE-125-d
CWE-89	Top 25	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	CWE-89-a
CWE-416	Top 25	Use After Free	CWE-416-a, CWE-416-b, CWE-416-c
CWE-190	Top 25	Integer Overflow or Wraparound	CWE-190-a, CWE-190-b, CWE-190-c, CWE-190-d, CWE-190-e, CWE-190-f, CWE-190-g
CWE-352	Top 25	Cross-Site Request Forgery (CSRF)	N/A
CWE-22	Top 25	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CWE-22-a
CWE-78	Top 25	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	CWE-78-a
CWE-787	Top 25	Out-of-bounds Write	CWE-787-a, CWE-787-b, CWE-787-c, CWE-787-d, CWE-787-e, CWE-787-f
CWE-287	Top 25	Improper Authentication	CWE-287-a
CWE-476	Top 25	NULL Pointer Dereference	CWE-476-a, CWE-476-b
CWE-732	Top 25	Incorrect Permission Assignment for Critical Resource	CWE-732-a, CWE-732-b
CWE-434	Top 25	Unrestricted Upload of File with Dangerous Type	N/A
CWE-611	Top 25	Improper Restriction of XML External Entity Reference	CWE-611-a
CWE-94	Top 25	Improper Control of Generation of Code ('Code Injection')	N/A

CWE-798	Top 25	Use of Hard-coded Credentials	CWE-798-a
CWE-400	Top 25	Uncontrolled Resource Consumption	CWE-400-a
CWE-772	Top 25	Missing Release of Resource after Effective Lifetime	CWE-772-a, CWE-772-b
CWE-426	Top 25	Untrusted Search Path	CWE-426-a
CWE-502	Top 25	Deserialization of Untrusted Data	N/A
CWE-269	Top 25	Improper Privilege Management	CWE-269-a, CWE-269-b
CWE-295	Top 25	Improper Certificate Validation	N/A
CWE-835	On the Cusp	Loop with Unreachable Exit Condition ('Infinite Loop')	CWE-835-a
CWE-522	On the Cusp	Insufficiently Protected Credentials	N/A
CWE-704	On the Cusp	Incorrect Type Conversion or Cast	CWE-704-a, CWE-704-b, CWE-704-c, CWE-704-d, CWE-704-e, CWE-704-f, CWE-704-g, CWE-704-h, CWE-704-i, CWE-704-j, CWE-704-k, CWE-704-l
CWE-362	On the Cusp	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	CWE-362-a, CWE-362-b, CWE-362-c, CWE-362-d, CWE-362-e
CWE-918	On the Cusp	Server-Side Request Forgery (SSRF)	N/A
CWE-415	On the Cusp	Double Free	CWE-415-a
CWE-601	On the Cusp	URL Redirection to Untrusted Site ('Open Redirect')	N/A
CWE-863	On the Cusp	Incorrect Authorization	CWE-863-a
CWE-862	On the Cusp	Missing Authorization	N/A
CWE-532	On the Cusp	Inclusion of Sensitive Information in Log Files	CWE-532-a
CWE-306	On the Cusp	Missing Authentication for Critical Function	N/A
CWE-384	On the Cusp	Session Fixation	N/A
CWE-326	On the Cusp	Inadequate Encryption Strength	CWE-326-a
CWE-770	On the Cusp	Allocation of Resources Without Limits or Throttling	CWE-770-a
CWE-617	On the Cusp	Reachable Assertion	CWE-617-a