MISRA C:2025 Addendum 5

Coverage of MISRA C:2025 against the Common Weakness Enumeration (CWE)

March 2025

First published March 2025 by The MISRA Consortium Limited
1 St James Court
Whitefriars
Norwich
Norfolk
NR3 1RU
UK

www.misra.org.uk

ISBN 978-1-911700-21-0 PDF

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library.

MISRA C:2025 Addendum 5

Coverage of MISRA C:2025 against the Common Weakness Enumeration (CWE)

March 2025

MISRA Mission Statement

MISRA provides world-leading best practice guidelines for the safe and secure application of both embedded control systems and standalone software.

MISRA is a collaboration between manufacturers, component suppliers, engineering consultancies and academics which seeks to research and promote best practice in developing safety- and security-related electronic systems and other software-intensive applications.

To this end, MISRA conducts research projects and publishes documents that provide accessible information for engineers and management.

MISRA also facilitates the dissemination and exchange of information between practitioners through supporting and holding technical events.

Foreword

Throughout the development of MISRA C, the main focus has been to address vulnerabilities in the C language, particularly for use in embedded systems, and primarily targeted at safety-related applications.

One of the great successes of MISRA C has been its adoption across many industries, and in environments where safety-criticality is less of a concern, but where data-security is more of an issue.

Increasingly, the Common Weakness Enumeration (CWE), administered by The MITRE Corporation, is being used as a reference for system weaknesses, whether hardware- or software- related, and irrespective as to the programming language used. Many of the enumerations will be relevant to high-integrity software written in C, and this document will map those that are covered by guidance within the MISRA C guidelines.

This first subset focusses on the weaknesses tagged as being relevant to memory safety (category CWE-1399), an area where some commentators are now suggesting makes the C programming language unsuitable for high-integrity software – the MISRA C Working Group respectfully disagrees with this assertion, and this document provides our evidence to support our position that C, with appropriate controls, provides a suitable language for developing safety- and security-related environments.

Future enhancements will extend the coverage to other CWE *categories* and *views.*

Andrew Banks FBCS CITP
Chairman, MISRA C Working Group

Acknowledgements

The MISRA C Working Group

The MISRA Consortium would like to thank the following members of the MISRA C Working Group for their significant contribution to the writing of this document:

Andrew Banks	LDRA Ltd (also Intuitive Consulting)
Roberto Bagnara	BUGSENG (and the University of Parma)
Jill Britton	Perforce
Chris Miller	GE Aerospace

The MISRA Consortium Limited also wishes to acknowledge contributions from the following individuals during the development and review process:

Chris Tapp	Keylevel Consultants
David Ward	HORIBA MIRA Limited

Other acknowledgements

DokuWiki was used extensively during the drafting of this document. Our thanks go to all those involved in its development.

This document was typeset using fonts licensed under the SIL Open Font License, Version 1.1:

- Open Sans — Copyright 2020, The Open Sans Project Authors
- Fira Code — Copyright 2014–2020, The Fira Code Project Authors

Contents

1 Introduction 1
- 1.1 Background 1
- 1.2 Glossary 1
- 1.3 Applicability 1

2 Glossary 2
- 2.1 Coverage classification 2
- 2.2 Coverage strength 2
- 2.3 Classes and Views 2

3 CWE cross reference 3
- 3.1 Guideline by guideline 3

4 Summary 5
- 4.1 Coverage summary 5
- 4.2 Scope summary 5

5 References 6
- 5.1 MISRA C 6
- 5.2 Other references 6

1 Introduction

1.1 Background

Throughout the development of MISRA C, the main focus has been to address vulnerabilities in the C language, particularly for use in embedded systems, and primarily targeted at safety-related applications.

One of the great successes of MISRA C has been its adoption across many industries, and in environments where safety-criticality is less of a concern, but where data-security is more of an issue.

Increasingly, the Common Weakness Enumeration (CWE), administered by The MITRE Corporation, is being used as a reference for system weaknesses, whether hardware- or software- related, and irrespective as to the programming language used. Many of the enumerations will be relevant to high-integrity software written in C, and this document will map those that are covered by guidance within the MISRA C guidelines.

1.2 Glossary

In this document:

- *Weakness* means a concern identified in the Common Weakness Enumeration (CWE)
- *MISRA C* means MISRA C:2025 *Guidelines for the use of the C language in critical systems* [1]

1.3 Applicability

This document provides a mapping of the weaknesses identified in the Common Weakness Enumeration (CWE) against MISRA C.

This document should be read in conjunction with MISRA C:2025 *Guidelines for the use of the C language in critical systems* [1]

2 Glossary

2.1 Coverage classification

The coverage of each weakness against MISRA C is classified as follows:

Status	Interpretation
Explicit	The weakness is EXPLICITLY covered by one or more MISRA C guidelines, which directly addresses the undesired behaviour.
Implicit	The weakness is IMPLICITLY covered by one or more MISRA C guidelines, although the behaviour is not explicitly referenced.
Restrictive	The weakness is covered by one or more MISRA C guidelines that prohibit a language feature in a RESTRICTIVE manner.
Partial	Some aspect of the weakness is covered by one or more MISRA C guidelines. However, some aspect of the weakness guideline is not covered by any MISRA C guideline.
None	The weakness is not covered by any MISRA C guideline.

2.2 Coverage strength

The strength of the coverage of each CERT C guideline against MISRA C is classified as follows:

Status	Interpretation
Strong	The weakness is covered by one or more targeted MISRA C guidelines.
Weak	The weakness is only covered by one or more MISRA C directives, or by Rule 1.3.
None	The weakness is not covered by any MISRA C guidelines.

Note: For weaknesses with Partial coverage, a combination of Strength coverages is shown.

2.3 Classes and Views

The coverage tables include highlighting membership of the following categories and classes:

CWE Category	
CWE-1399	Memory Safety
CWE Classes	
CWE-0119	Improper Restriction of Operations within the Bounds of a Memory Buffer

3 CWE cross reference

3.1 Guideline by guideline

CWE	Category	MISRA C Guidelines	MISRA C Coverage		119	1399	Comments
			Coverage	Strength			
CWE-0119	Class	R.9.1 + R.11.1-6 + R.18.1 + R.21.6/21.17/21.18 + R.22.2 + D.4.7/4.11 + R.1.3	Collection	Strong	-	X	-
CWE-0120	Base	R.18.1 + R.21.6/21.17/21.18 + R.1.3	Implicit	Strong	X	X	-
CWE-0121	Variant	R.18.1 + R.21.6/21.17/21.18 + R.1.3	Implicit	Strong	-	X	-
CWE-0122	Variant	R.18.1 + R.21.6/21.17/21.18 + R.1.3	Implicit	Strong	-	X	-
CWE-0123	Base	R.18.1 + R.21.6/21.17/21.18 + R.1.3	Implicit	Strong	X	X	-
CWE-0124	Base	R.18.1 + R.21.6/21.17/21.18 + R.1.3	Implicit	Strong	-	X	-
CWE-0125	Base	R.18.1 + R.21.6/21.17/21.18 + R.1.3	Implicit	Strong	X	X	-
CWE-0126	Variant	R.18.1 + R.21.6/21.17/21.18 + R.1.3	Implicit	Strong	-	X	-
CWE-0127	Variant	R.18.1 + R.21.6/21.17/21.18 + R.1.3	Implicit	Strong	-	X	-
CWE-0129	Variant	R.18.1 + R.21.6/21.17/21.18 + R.1.3 + D.4.1	Implicit	Strong	-	X	-
CWE-0130	Base	R.21.18 + D.4.11	Implicit	Strong	X	I	-
CWE-0131	Base	R.18.1 + R.21.6/21.17/21.18 + R.1.3	Implicit	Strong	-	X	-
CWE-0134	Base	R.21.6 + D.4.11/4.14	Restrictive	Strong	-	X	-
CWE-0188	Base	R.19.2 + D.1.1	Partial/Restrictive	Strong	-	X	-
CWE-0190	Base	D.4.1	Implicit	Weak	-	I	See 0680
CWE-0198	Variant	D.1.1	Implicit	Weak	-	X	-
CWE-0244	Variant	R.21.3 + D.4.1/D.4.12 + R.1.3	Partial/Restrictive	Strong	-	X	-
CWE-0252	Base	D.4.7	Implicit	Weak	-	I	See 0690
CWE-0401	Variant	R.22.2 + D.4.1/D.4.12 + R.1.3	Partial/Restrictive	Strong	-	X	-
CWE-0415	Variant	R.22.2 + D.4.1/D.4.12 + R.1.3	Partial/Restrictive	Strong	-	X	-
CWE-0416	Variant	R.22.2 + D.4.1/D.4.12 + R.1.3	Partial/Restrictive	Strong	-	X	-
CWE-0466	Base	R.18.1	Implicit	Strong	X	X	-

CWE	Category	MISRA C Guidelines	MISRA C Coverage		119	1399	Comments
			Coverage	Strength			
CWE-0476	Base	D.4.1	Implicit	Weak	-	I	See 0690
CWE-0562	Base	R.18.9	Explicit	Strong	-	X	-
CWE-0587	Variant	R.11.4	Explicit	Strong	-	X	-
CWE-0590	Variant	R.22.2	Explicit	Strong	-	X	-
CWE-0680	Compound	R.9.1 + R.11.1-6 + R.18.1 + R.21.6/21.17/21.18 + R.22.2 + D4.1/4.7/4.11 + R.1.3	Collection	Strong	-	X	0190+0119
CWE-0690	Compound	D.4.1/4.7	Collection	Weak	-	X	0252+0476
CWE-0761	Variant	R.22.2	Explicit	Strong	-	X	-
CWE-0762	Variant	R.22.2 + D.4.13	Explicit	Strong	-	X	-
CWE-0763	Base	R.22.2	Explicit	Strong	-	X	-
CWE-0786	Base	R.18.1	Explicit	Strong	X	X	-
CWE-0787	Base	R.18.1 + R.21.6/21.17/21.18	Partial/Restrictive	Strong	X	X	-
CWE-0788	Base	R.18.1 + R.21.6/21.17/21.18	Partial/Restrictive	Strong	X	X	-
CWE-0789	Variant	R.21.18 + R.21.3 + D.4.1/4.12 + R.1.3	Partial/Restrictive	Strong	-	X	-
CWE-0805	Base	R.21.18 + D.4.11	Implicit	Strong	X	X	-
CWE-0806	Variant	R.21.17/21.18 + D.4.1	Implicit	Strong	-	X	-
CWE-0822	Base	R.11.1-6 + D.4.7/4.14	Explicit	Strong	X	X	-
CWE-0823	Base	R.18.1	Explicit	Strong	X	X	-
CWE-0824	Base	R.9.1	Explicit	Strong	X	X	-
CWE-0825	Base	R.22.2 + R.1.3	Implicit	Strong	X	X	-
CWE-1399	Category	Aggregate	Collection	Strong	-	-	-

4 Summary

4.1 Coverage summary

In summary, the coverage of MISRA C against the CWE is as follows:

MISRA C Coverage		
Coverage	Strength	Number
Collection	Strong	3
	Weak	1
Explicit	Strong	10
	Weak	0
Implicit	Strong	15
	Weak	4
Restrictive	Strong	1
	Weak	0
Partial Restrictive	Strong	8
	Weak	0
Sub-total		42
None	None	0
Total		42

4.2 Scope summary

For completeness, the coverage of MISRA C against the CWE is assessed as follows:

MISRA C Coverage		
CWE Category	Covered	of Total
Base	22	525
Variant	16	290
Class	1	108
Compound	2	7
Pillar	0	10
Subtotal	41	940
Category	1	374
View	0	51
Total current	42	1,365
Deprecated	0	64
Total	42	1,429

5 References

5.1 MISRA C

[1] MISRA C:2025 *Guidelines for the use of the C language in critical systems*
ISBN 978-1-911700-19-7 (paperback), ISBN 978-1-911700-20-3 (PDF),
The MISRA Consortium Limited, Norwich, March 2025

5.2 Other references

[2] The *Common Weakness Enumeration* v4.16 (November 2024)
Accessed via https://cwe.mitre.org/
Operated by The MITRE Corporation