WG14 Document: N1578

September 23, 2011

C Secure Coding Rules Editor's Report

1. Status

N1579 is the first submission of this document so all the content is new. N1579 was derived from "The CERT C Secure Coding Standard" which was reviewed by the committee at the London (2007), Kona (2007), and Delft (2008) meetings but was substantially revised by the C Secure Coding Rules (CSGR) study group over the 2 years of the study group's existence.

2. Open Issues

There are some open issues that still need to be addressed in subsequent revisions to N1579.

The following rules need to be reviewed and possibly revised to address taint analysis:

- Using tainted integer values in taintedness sinks (INT04-C)
- Use of an implied default in a switch statement (MSC01-C)
- Converting an integer to a type which is unable to represent its value (INT31-C)
- Converting floating point values to types that cannot represent their value (FLP34-C)

The following rules require some revision for clarity/precision:

- Failing to close files or free dynamic memory when they are no longer needed (FIO42-C)
- Comparison of padding data (EXP04-C)

The following rules need compliant examples:

- Dereferencing a null pointer (EXP34-C)
- Comparing or assigning expressions to a larger size objects (INT35-C)
- Assigning in conditional expressions (EXP18-C)
- Conversion of signed characters to wider integer types (STR34-C)

Use of an implied default in a switch statement (MSC01-C) may be narrowed to apply only to `enum` types.

Assuming character data does not contain a null byte (FIO37-C) may be redundant with other rules and eliminated.