2.3.1. Exploitability assessment

(Last updated: 2017/01/23)

The exploitability assessment is based on the CVSSv2 scoring system and considers the following (See http://www.first.org/cvss/cvss-guide.html#i2.1 for more information on these metrics):

1. **Authentication**: Is authentication needed or not?
2. **Complexity**: How complex (high, medium, or low) is it to exploit the vulnerability?
3. **Accessibility**: What level of access (local, adjacent network, or network) is needed to exploit the vulnerability?

The following matrix shall be used for this exploitability assessment (see http://www.first.org/cvss/cvss-guide.html#i3.2 for more information about how the score has been calculated):

access	complexity	authentication	score	Exploitability level
Local	high	needed	1,5	LOW (HARD)
Local	high	not needed	1,9	LOW (HARD)
Local	medium	needed	2,7	LOW (HARD)
Local	medium	not needed	3,4	LOW (HARD)
Local	low	needed	3,1	LOW (HARD)
Local	low	not needed	3,9	MEDIUM
adjacent	high	needed	2,5	LOW (HARD)
adjacent	high	not needed	3,2	LOW (HARD)
adjacent	medium	needed	4,4	MEDIUM
adjacent	medium	not needed	5,5	MEDIUM
adjacent	low	needed	5,1	MEDIUM
adjacent	low	not needed	6,5	HIGH (EASY)
any	high	needed	3,9	MEDIUM
any	high	not needed	4,9	MEDIUM
any	medium	needed	6,8	HIGH (EASY)
any	medium	not needed	8,6	HIGH (EASY)
any	low	needed	8,0	HIGH (EASY)
any	low	not needed	10,0	HIGH (EASY)

The person performing the exploitability assessment shall document his finding in the ticket.