**Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)**

*Please submit responses to dig-comments@nist.gov by March 24, 2023*

| | |
|---|---|
| ***Organization:*** | *Taproot Security* |
| ***Name of Submitter/POC:*** | *Michael McCormick* |
| ***Email Address of Submitter/POC:*** | [REMOVED] |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| 1 | 63B | 5.1.1.2 | 15 | 712 | Dictionary words on the blocklist should include case variations (password, Password, PASSword, ...) as well as numeric suffixes (passsword1, password235, ...) and "leet" substitutions (passw0rd, pa55word, ...). | |
| 2 | 63B | 5.1.4.1 | 24 | 966 | The secret key must be unique to the OTP device | |
| 3 | 63B | 5.1.4.2 | 25 | 994 | The degree of permissible clock drift should not exceed 2 minutes. Large skew windows increase risk of replay attacks. | |
| 4 | 63B | 5.1.5.1 | 25 | 1020 | The secret key must be unique to the MF-OTP device | |
| 5 | 63B | 5.1.5.2 | 26 | 1060 | The degree of permissible clock drift should not exceed 2 minutes. Large skew windows increase risk of replay attacks. | |
| 6 | 63B | 5.2.2 | 31 | 1235 | Allowing 100 consecutive authentication failures is excessive, far greater than most organizations' policies or industry best practice. 10 would be reasonable. | |
| 7 | 63B | 5.2.3 | 33 | 1280 | Rather than a blanket FMR limit of 1:10000, a different limit should be specified for each EAL. | |
| 8 | 63B | 7.1.3 | 50 | 1881 | Device fingerprinting - as opposed to true unique device identification - must not be used to enact a session. Device fingerprints are typically profiles aggregated from attributes such as OS version, browser version, screen resolution, etc. that are not adequately unique for authentication usage. | |
| 9 | 63B | 8.4 | 58 | 1973 | An often overlooked session defense is to make explicit logoff easy for the user. Ensure a logoff button or menu selection is prominent on every screen. Educate users to log off applications when finished. Logoffs reduce opportunities for session hijacks including XSS and CSRF. | |
| 10 | 63B | 10.1 | 63 | 2134 | User facing text or images should not include icons such as padlocks or shields that typically serve as security indicators in browser chrome. Users can easily confuse page display with chrome. | |
| 11 | 63B | 10.3 | 69 | 2359 | There is no discussion in clause 10 of usability considerations for session management. At minimum, the need for easy-to-find logoff should be mentioned. (see comment 9) | |
| 12 | 63B | 10.4 | 72 | 2394 | Some users do not have fingers. While this may be considered an accessibility issue, it does mean alternative means of authentication may be needed for such users, along with those whose fingerprints have been severely degraded. | |