WEAKNESS

ACCESS AND OUT-OF-BOUNDS READ #125, #126, #127, #786

FAILURE TO CONSTRAIN OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER #119

IMPROPER-ACCESS-OF-INDEXABLE-RESOURCE #118

[Change Log Issue Description]: Off-by-one error in the toAlphabetic function in rendering/RenderListMarker.cpp

[Change Log Fix Description]: We need to decrement numberShadow rather than subtracting one from the result of the modulo operation

[Code Change for Fix]: Line 105 decrement (--numberShadow) and remove the subtraction of one in Line 106 (sequence[numberShadow % sequenceSize];)

CONSEQUENCES

WRITE-WHAT-WHERE CONDITION #123

[CVE Description]: ....allows remote attackers to obtain sensitive information...

[Chrome Release Announcement]: ....Memory corruption in rendering....

[Chrome Release Announcement]: ....This is a security fix for memory corruption in rendering....

[Change Log Issue Description]: ....trying to access an array at index -1 in some cases

[Change Log Fix Description]: We need to decrement numberShadow rather than subtracting one from the result of the modulo operation

[Code]: Missing validation of array size in Line 106 (sequence[numberShadow % sequenceSize];)

[CVE Description]: Off-by-one error in the toAlphabetic function in rendering/RenderListMarker.cpp

[Change Log Issue Description]: The math was slightly off here, and we wound up trying to access an array at index -1 in some cases

[Change Log Fix Description]: We need to decrement numberShadow rather than subtracting one from the result of the modulo operation

[Code Change for Fix]: Line 105 decrement (--numberShadow) and remove the subtraction of one in Line 106 (sequence[numberShadow % sequenceSize];)