Common Vulnerabilities and Exposures

CVE-2018-90017117

Also known as: #KingMe attack

Published 2018-12-03

Partial embargo until 2019-04-01

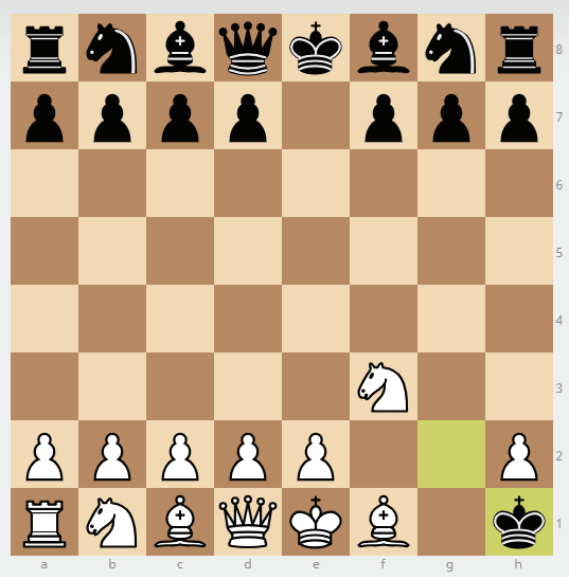
Reported by t0m7 of East Coast Hacking Organization

Description

An input validation error in the move parser allows remote privilege escalation.

Background

The popular internet chess site lichess.org allows for the import of PGN files, a standard text-based interchange format for giving the sequence of moves in a game. Moves look like “e4” (move a pawn to the e4 square) or “Qxd3” (queen captures on d3) or “Rcc8” (the rook on the C file moves to c8). When a pawn moves into the last or first rank, it usually promotes to queen, but may legally promote to a bishop, knight, or rook at the player’s option. This preference is specified using the notation g8=B (or N for knight, R for rook, or Q for queen to optionally be explicit). lichess.org does not properly implement this syntax, and allows a move like g8=K, which is not legal chess.



Screenshot. After 5. ... gxh1=K ?!, black promotes their g pawn to a second king.

Impact

The pawn is promoted to a king. This is a privilege escalation vulnerability, because the king has privileges that the pawn does not have, such as the privilege to be checkmated.

Scope

The issue is only confirmed during PGN import (e.g. in “analysis board”). In live games, it is possible to use keyboard entry of moves in PGN notation, but =K is ignored. It is possible that these moves are only rejected in the frontend and would be allowed by the underlying chess engine (if made directly through the API, for example). After a second king is introduced, the game appears to be quite broken; some parts of the interface behave as though the game is a draw and no further moves are allowed, but the computer continues to suggest lines in the background. When evaluating this vulnerability in other systems, note that the king has not yet moved, and so could erroneously be considered eligible to castle (e.g. with the h8 rook), a potential 0-0-day.

Example exploit

1. f4 e5 2. Nf3 exf4 3. g4 fxg3 4. Ng1 g2 5. Nf3 gxh1=K

Classification - Office Use Only

```
CVSS v3.0 Severity and Metrics:
Base Score: 7.7 HIGH
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N (V3 legend)
Impact Score: 7.9
Exploitability Score: 8.9
```