Alert Bulletin

Bulletin N.: 2024-01
Publication Date: 09/01/2024
Subject: Alert 2024-01 Terrapin attack affecting SSH protocol
Traffic Light Protocol (TLP): White

A new attack affecting the SSH remote connection standard has been reported, developed by academic researchers at Ruhr University Bochum, who developed a new attack called Terrapin that manipulates sequence numbers during the handshake process to break the integrity of the SSH channel when certain widely used encryption modes are used. The weaknesses and flaws associated with the attack are identified as CVE-2023-48795, CVE-2023-46445 and CVE-2023-46446.