OpenSSL-lek maakt webservers kwetsbaar voor dos-aanvallen

Een **beveiligingslek in OpenSSL** maakt webservers kwetsbaar voor denial of service (dos)-aanvallen, zo waarschuwen de ontwikkelaars die een beveiligingsupdate hebben uitgebracht. OpenSSL behoort tot de meest gebruikte software voor het versleutelen van internetverbindingen.

Websites maken er bijvoorbeeld gebruik van om het verkeer van en naar bezoekers te versleutelen. De kwetsbaarheid zorgt ervoor dat server- of clientapplicaties die van OpenSSL gebruikmaken en tijdens of na een TLS 1.3-handshake een specifieke functie aanroepen, door het versturen van een ongeldig handtekeningsalgoritme zijn te laten crashen. Hierdoor zou een aanvaller een remote dos-aanval op webservers kunnen uitvoeren.

De kwetsbaarheid is aanwezig in **OpenSSL** versie 1.1.1d, 1.1.1e en 1.1.1f en is verholpen in 1.1.1g. OpenSSL-versies 1.1.1c en ouder zijn niet kwetsbaar. OpenSSL kent vier niveaus om de impact van kwetsbaarheden te beoordelen: low, moderate, high en critical. Deze kwetsbaarheid is als "high" beoordeeld, wat al meer dan drie jaar niet is voorkomen. Alle gevonden beveiligingslekken in de afgelopen drie jaar kregen het stempel low of moderate.