Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0341

Kwetsbaarheden verholpen in BIND 9

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 24-10-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

ISC heeft kwetsbaarheden verholpen in BIND 9 (Specifiek voor versies 9.16.0 tot 9.16.50, 9.18.0 tot 9.18.39, 9.20.0 tot 9.20.13, en 9.21.0 tot 9.21.12).

Duiding

De kwetsbaarheden bevinden zich in de DNS-resolvers van BIND 9. De eerste kwetsbaarheid stelt aanvallers in staat om vervalste DNS-records in de cache te injecteren, wat kan leiden tot het omleiden van clients naar kwaadaardige domeinen. Een tweede kwetsbaarheid is gerelateerd aan een zwakte in de Pseudo Random Number Generator (PRNG), waardoor aanvallers bronpoorten en query-ID's kunnen voorspellen, wat kan leiden tot cache poisoning aanvallen. De derde kwetsbaarheid laat ongeauthenticeerde aanvallers toe om misvormde DNSKEY-records te verzenden, wat resulteert in aanzienlijke CPU-uitputting en kan leiden tot een denial-of-service voor legitieme clients. Deze kwetsbaarheden zijn vooral zorgwekkend voor omgevingen die afhankelijk zijn van de specifieke versies van BIND 9.

Oplossingen

ISC heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://kb.isc.org/docs/cve-2025-40778
- https://kb.isc.org/docs/cve-2025-40780
- https://kb.isc.org/docs/cve-2025-8677

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-40778	8.6 HIGH
CVE-2025-40780	8.6 HIGH
CVE-2025-8677	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
CWE-341	Predictable from Observable State
CWE-347	Improper Verification of Cryptographic Signature
CWE-349	Acceptance of Extraneous Untrusted Data With Trusted Data
CWE-400	Uncontrolled Resource Consumption
CWE-405	Asymmetric Resource Consumption (Amplification)

Getroffen producten

ISC
BIND 9

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.