

Nokian N95 kaadettavissa sip-paketeilla

7.12.2007 09:40 — Matias Mäki matias.maki@sanoma.fi

Nokian N95-älypuhelimien sip (session initiation protocol) -toteutuksesta on löydetty palvelunestohaavoittuvuus ja sille on julkaistu hyväksikäyttömenetelmä. Vika saattaa koskea myös muita Nokian puhelinmalleja.

Ranskalainen Madyness -tietoturvatutkimustiimi on löytänyt Nokian N95-älypuhelimien ohjelmiston vanhasta 12.0.013 -versiosta sip-toteutuksen vähäisen haavoittuvuuden. Tutkijoiden mukaan myös laitteen muut ohjelmistoversiot ja Nokian muut puhelinmallit saattavat kärsiä haavoittuvuudesta.

Haavoittuvuus johtuu sip-viestien prosessoinnista löytyvästä heikkoudesta, jota hyödyntämällä puhelin saadaan jumiutettua. Haavoittuvuuden hyödyntäminen vaatii sip-toiminnallisuuden päällä oloa ja haitalliseksi muokattujen sip-pakettien lähettämistä kohdepuhelimelle.

Tutkijat löysivät haavoittuvuuden jo syyskuun puolivälissä. He ilmoittivat asiasta Nokialle kahteen otteeseen, eivätkä ole saaneet mitään vastausta raporttiinsa. Nyt he kuitenkin julkaisivat [tietoturvatiedotteen ja haavoittuvuuden hyväksikäyttömenetelmän Full Disclosure -postituslistalla](#) Tietoturvayhtiö Secunia on luokitellut haavoittuvuuden hyvin vähäiseksi ongelmaksi.

<http://www.digitoday.fi/tietoturva/2007/12/07/nokian-n95-kaadettavissa-sip-paketeilla/200731059/66>