

Siemensin teollisuussoftaan hyökätään

20.7.2010 10:15

Cert-fi kertoi tarkempia tietoja uuden Windows-haavoittuvuuden hyväksikäytöstä. Iskun kohteeksi on joutunut Siemensin tehdasohjelmisto, jonka salasana on ilmeisesti vuotanut ulos.

Viestintäviraston tietoturveysikkö [Cert-fi väivitti tietojaan](#) Windowsin korjaamattomasta haavoittuvuudesta pikakuvakkeiden käsittelyssä. Yksikön mukaan hyökkäyksiä tehdään Siemensin teollisuusautomaatiojärjestelmiin.

Siemensin Simatic WinCC - ja Step7 -ohjelmistoissa on tietoturvaheikkous, jota käytetään hyväksi yhdessä Windows-aukon kanssa. Motiivina voi olla teollisuusvakoilu; esimerkiksi prosessiteollisuudessa Simatic-järjestelmään saattaa olla tallennettuna valmistettavan tuotteen kokoonpano ja valmistusresepti, Cert-fi huomauttaa.

Oletussalasanana pääsi karkuun

Hyökkäysten yhteyden Simatic-järjestelmiin havaitsi tietoturvatutkija **Frank Boldewin**. Hän huomasi haittaohjelman tekevän "kummallisia hakuja WinCC- + S7-tietokantaan".

Cert-fi:n mukaan WinCC-järjestelmän kaikissa ohjelmistokokoonpanoissa on niin sanottu takaportti. Syynä siihen on ilmeisesti julkisuuteen päässyt salasana, jota käytetään tietokantayhteyden muodostukseen kaikissa asennetuissa WinCC-järjestelmissä.

Tämä oletusarvoinen salasana ei ole käyttäjän vaihdettavissa ilman järjestelmän toiminnan vaarantumista. Siemens on ilmoittanut laativansa asiasta tiedonannon asiakkailleen. Tiedonanto ei ole Cert-fi:n käytettävissä.

Leviää usb-muisteilla

[Microsoft on tiedottanut](#) Windowsin pikakuvakeaukosta, johon isketään [minkin usb-massamuistien avulla](#). Yhtiö on valmistamassa korjausta haavoittuvuuteen, mutta aikataulu on epäselvä.

Tällainen hyökkäystapa on tuttu esimerkiksi Conficker-madosta, joka levisi lisäksi verkossa madon tavoin.

Cert-fi:n mukaan Windowsin autorun/autoplay-toiminnon estäminen ei suojaa saastumiselta.

Saastumisen voi välttää huolehtimalla virustorjunnan ajantasaisuudesta ja tarkistamalla tietokoneeseen liitettävät ulkoiset mediat. Teollisuusautomaatiojärjestelmän eristäminen julkisesta verkosta ei riitä, jos järjestelmään tai sen yhteydessä oleviin tietokoneisiin saa liittää ulkopuolisia massamuisteja.

Hyökkäyksiä on havaittu pääasiassa Aasiassa, mutta Cert-fi on ollut yhteydessä suomalaisiin huoltovarmuuskriittisiin toimijoihin asian tiimoilta.

Kirjoittaja: Tuomas Linnake
tuomas.linnake@digitoday.fi

<http://www.itviikko.fi/uutiset/2010/07/20/siemensin-teollisuussoftaan-hyokataan/20109991/7>