

Re: [Full-Disclosure] 2 vulnerabilities combine to auto execute received files in Nokia series 60 OS

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-01/0811.html>

From: Thierry Zoller (Thierry_at_sniff-em.com)

Date: 01/24/05

Date: Mon, 24 Jan 2005 21:11:16 +0100

To: "Paul Kurczaba" <seclists@securinews.com>

Dear Paul Kurczaba,

PK> Wouldn't the phone try to open the jpg file as a picture, and not execute
PK> it. Just like on desktop PCs: if you rename a .exe (application/program) to
PK> a jpg (picture file), and try to open the file, your image program will open
PK> the file, thinking it is a image file. The application code will not be
PK> executed.

Well there is a twist, Nokia says it identifies files NOT by the filename but by the extension, even when shelling them, so there won't be an image view but code being run. (Note I have no access to said devices, I am solely interpreting).

--

Regards,

Thierry Zoller

<http://www.sniff-em.com> [Yes]

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>