

n.runs AG
http://www.nruns.com/
n.runs-SA-2007.017

security(at)nruns.com
20-Jul-2007

Vendor: ESET, <http://eset.com>
Affected Products: ESET NOD32 Antivirus
Vulnerability: Denial of Service (remote)
Risk: MODERATE

Vendor communication:

2007/05/07	Initial notification to ESET
2007/05/07	ESET Response
2007/05/07	PoC files sent to ESET
2007/05/10	ESET validate the vulnerability
2007/05/24	ESET made available the updates

Overview:

Founded in 1992, ESET is a global provider of security software for enterprises and consumers. ESET's award-winning, antivirus software system, NOD32, provides real-time protection from known and unknown viruses, spyware, rootkits and other malware. NOD32 offers the smallest, fastest and most advanced protection available, with more Virus Bulletin 100% Awards than any other antivirus product. ESET was named to Deloitte's Technology Fast 500 five years running, and has an extensive partner network, including corporations like Canon, Dell and Microsoft. ESET has offices in Bratislava, SK; Bristol, U.K.; Buenos Aires, AR; Prague, CZ; San Diego, USA; and is represented worldwide in more than 100 countries. The broad product platform protects Windows, Linux, Novell and MS DOS machines.

Description:

A remotely exploitable vulnerability has been found in the file parsing engine.

In detail, the following flaw was determined:

- Infinite Loop through Integer Overflow in ASPACK packed files parsing

Impact:

This problem can lead to remote denial of service provoked by high CPU consume and exhaustion of storage resource if an attacker carefully crafts a file that exploits the aforementioned vulnerability. The vulnerability is present in NOD32 Antivirus software versions prior to the update v.2.2289.

Solution:

The vulnerability was reported on May 07 and an update has been issued on May 24 to solve this vulnerability through the regular update mechanism.

Credit:

Bugs found by Sergio Alvarez of n.runs AG.

References:

http://www.eset.com/joomla/index.php?option=com_content&task=view&id=3469&Itemid=26

This Advisory and Upcoming Advisories:
http://www.nruns.com/security_advisory.php
<http://www.nruns.com/parsing-engines-advisories.php>

Unaltered electronic reproduction of this advisory is permitted. For all other reproduction or publication, in printing or otherwise, contact security@nruns.com for permission. Use of the advisory constitutes acceptance for use in an "as is" condition. All warranties are excluded. In no event shall n.runs be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if n.runs has been advised of the possibility of such damages.

Copyright 2007 n.runs AG. All rights reserved. Terms of apply.