

n.runs AG  
http://www.nruns.com/  
n.runs-SA-2007.021

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

---

Vendor: Norman, http://www.norman.com  
Affected Products: All Norman Antivirus Solutions  
Vulnerability: Arbitrary Code Execution (remote)  
Risk: CRITICAL

---

Vendor communication:

2007/05/07 Initial notification to Norman together with our RFP  
2007/05/08 Norman Responses asking for the PoC files  
2007/05/08 Request public PGP keys  
2007/05/08 PGP keys exchange  
2007/05/08 PoC files sent to Norman  
2007/05/08 Norman has PGP incompatible version problems  
2007/05/08 Norman requests n.runs to send the PoC files RAR'ed  
with password sent in in a separate mail  
2007/05/08 Send the PoC files RAR'ed with password.  
2007/05/08 Send the RAR'ed files password.  
2007/05/08 Norman validates the vulnerabilities and informs that  
the vulnerabilities will take long QA process because  
the update for this vulnerabilities will need system  
reboot.  
2007/05/09 n.runs thanks for the feedback and asks for an  
estimation of time to fix the vulnerabilities  
2007/05/23 Ping Norman for a replay  
2007/05/23 Norman replays that has forwarded the PoC files to  
their engine/unpacker programmers, but hasn't  
received any update as to how fast these can be fixed.  
2007/05/23 n.runs thanks Norman for the feedback and reminds to  
keep aligned with n.runs RFP (for the delay in the  
replay)  
2007/06/19 Ping to Norman for update on fix status and reminds  
that the communication have to be aligned with  
n.runs RFP  
2007/06/19 Norman replays that can't decrypt the last mail (the  
PING mail of the same date) and that has generated a  
new DH/DSS key to use.  
2007/06/19 Re-Send the Ping to Norman for status update  
encrypted with the new Norman's key  
2007/07/05 n.runs requests a replay to the ping In Clear Text  
including the before mentioned PING mails as the  
contents have no sensitive information.  
2007/07/05 Norman replays and acknowledges that has received the  
previous PING mail and adds the "Head of Engine  
Development Team" in the loop.  
2007/07/05 Norman's "Head of Engine Development Team" replays  
that The OLE2 issues should be resolved with the  
latest scanner engine (5.91.02) and that the  
decompression issues, the crash cases will be  
resolved soon, and he would expect an update to be  
available within the next month  
2007/07/05 n.runs thanks for the update information, also asks  
how the credits are going to be handled and reminds  
that the communication have to be aligned with  
n.runs RFP  
2007/07/10 Norman replays the following:

"Sergio,

We have discussed your mail. It is not our company's policy

to publish information about vulnerabilities or bugs in our software, unless they are extremely critical and/or can be worked around by the end-user. There are usually a large number of vulnerabilities/bugs in any software, and in our opinion it would only serve to unsettle user confidence in the products if the industry continually feeds information about such weaknesses, and we don't see that it would give the user any benefit in return.

Instead we feel that it should be the supplier's responsibility to correct any errors and weaknesses and have them released to the user fast and silently, without alerting also the malware industry.

Hence, there is no forum where we can credit you for your findings.

We sincerely appreciate that you notify us whenever you find a vulnerability in our software, as we appreciate such information from other sources. These findings, in addition to bug reports, are continuously being reviewed with respect to seriousness and work involved in fixing the problems, and assigned priorities accordingly, but no estimated dates for fixing the issues are published.

This has always been - and presently is - our company's policy. This policy may of course be revised by company management at any time, if deemed necessary or useful."

2007/07/11	n.runs replays that when they request the PoC files they implicitly accepted n.runs RFP and that the last mail was violating n.runs RFP and request a soon replay, otherwise the advisories would have to be release uncoordinated.
2007/07/23	Norman DID NOT replay
2007/07/23	n.runs assumes that Norman finalized their communication with n.runs
2007/07/23	Advisories release

---

#### Overview:

Norman ASA is a world leading company within the field of data security, internet protection and analysis tools. Through its SandBox technology Norman offers a unique and proactive protection unlike any other competitor.

While focusing on its proactive antivirus technology, the company has formed alliances which enable Norman to offer a complete range of data security services.

Norman was established in 1984 and is headquartered in Norway with continental Europe, UK and US as its main markets.

#### Description:

Multiple remotely exploitable vulnerabilities have been found in the file parsing engine.

In detail, the following flaw was determined:

- 3 (Three) Buffer Overflow through Integer Cast Around in .LZH file parsing

Impact:

These problems can lead to remote arbitrary code execution if an attacker carefully crafts a file that exploits any of the aforementioned vulnerabilities. The vulnerabilities are present in Norman Antivirus software since at least version 5.90.

Solution:

These vulnerabilities were reported on May 07 and may remain UNFIXED to the current date 23.Jul.2007.

---

Credit:

Bugs found by Sergio Alvarez of n.runs AG.

---

References:

This Advisory and Upcoming Advisories:

[http://www.nruns.com/security\\_advisory.php](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](mailto: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.