



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

December 23, 2008

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

STATE OF ALASKA ADVISORY NUMBER:

2008-032

DATE(S) ISSUED:

12/23/2008

SUBJECT:

Vulnerability in SQL Server Could Allow Remote Code Execution

OVERVIEW:

By calling the extended stored procedure `sp_replwritetovarbin`, and supplying several uninitialized variables as parameters, it is possible to trigger a memory write to a controlled location. Depending on the underlying Windows version, it is / may be possible to use this vulnerability to execute arbitrary code in the context of the vulnerable SQL server process.

In a default configuration, the `sp_replwritetovarbin` stored procedure is accessible by anyone. The vulnerability can be exploited by an authenticated user with a direct database connection, or via SQL injection in a vulnerable web application.

SYSTEMS AFFECTED:

- Microsoft SQL Server 2000 Service Pack 4 (incl. Itanium)
- Microsoft SQL Server 2005 Service Pack 2 (incl. x64 and Itanium)
- Microsoft SQL Server 2005 Express Edition Service Pack 2
- Microsoft SQL Server 2005 Express Edition with Advanced Services SP 2
- Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) Service Pack 4
- Microsoft SQL Server 2000 Desktop Engine (WMSDE)
- Windows Internal Database (WYukon) Service Pack 2

NON-AFFECTED SYSTEMS:

- Microsoft SQL Server 7.0 Service Pack 4
- Microsoft SQL Server 2005 Service Pack 3 (incl. x64 and Itanium)
- Microsoft SQL Server 2008 (incl. x64 and Itanium)

RISK:

Government:

- Large and medium government entities: **Low**
- Small government entities: **Low**

Businesses:

- Large and medium business entities: **Low**
- Small business entities: **Low**

Home users: Low

DESCRIPTION:

By calling the extended stored procedure `sp_replwritetovarbin`, and supplying several uninitialized variables as parameters, it is possible to trigger a memory write to a controlled location. Depending on the underlying Windows version, it is / may be possible to use this vulnerability to execute arbitrary code in the context of the vulnerable SQL server process.

In a default configuration, the `sp_replwritetovarbin` stored procedure is accessible by anyone. The vulnerability can be exploited by an authenticated user with a direct database connection, or via SQL injection in a vulnerable web application.

This triggers an access violation exception (write to address 0x41414141).

The vulnerability has been successfully used to execute arbitrary code on a lab machine.

RECOMMENDATIONS:

Microsoft recommend the following actions be taken:

Remove the `sp_replwritetovarbin` extended stored procedure. Run the following as an administrator:

```
execute dbo.sp_dropextendedproc 'sp_replwritetovarbin'
```

See also:

"Removing an Extended Stored Procedure from SQL Server"
[http://msdn.microsoft.com/en-us/library/aa215995\(SQL.80\).aspx](http://msdn.microsoft.com/en-us/library/aa215995(SQL.80).aspx)

REFERENCES:

SEC:

http://www.sec-consult.com/files/20081209_mssql-sp_replwritetovarbin_memwrite.txt

Microsoft:

<http://www.microsoft.com/technet/security/advisory/961040.mspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4270>