

[NT] Sun ONE (iPlanet) Application Server Connector Module Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0036.html>

From: support@securiteam.com

Date: 03/16/03

From: support@securiteam.com

To: list@securiteam.com

Date: 16 Mar 2003 14:38:55 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Sun ONE (iPlanet) Application Server Connector Module Overflow

SUMMARY

A stack buffer overflow exists in the Connector Module that ship with the Sun ONE Application Server. The module is an NSAPI plugin that integrates the Sun ONE Web Server (formerly iPlanet Enterprise Server) with the Application Server. Incoming HTTP request URLs are handled by the module and an unbounded string operation causes the overflow.

This is a classic stack buffer overflow and a remote attacker can gain control of the running web server.

DETAILS

Vulnerable systems:

* SunONE (iPlanet) Application Server version 6.x (Microsoft Windows (NT 4.0/2000))

The gxnsapi6.dll module that ships with the Sun ONE application server uses a static buffer in the handling of the incoming request URI.

Securiteam: [NT] Sun ONE (iPlanet) Application Server Connector Module Overflow

An overly long request URI in the form of `/[AppServerPrefix]/[long buffer]` will cause the overflow. The condition is exploitable as the saved EIP register is overwritten.

Vendor Response:

The vendor was initially contacted via email on 5/22/2002.

Vendor has a patch available for Sun One Application Server 6.5. Download SP1 at:

<<http://www.sun.com/software/download/products/3e3afb89.html>>
<http://www.sun.com/software/download/products/3e3afb89.html>

Vendor has no patch available for version 6.0. Queries to the vendor as to the best solution for 6.0 customers were not answered.

Recommendation:

If you are using version 6.5 you should and you are able to patch your server you should apply SP1.

We offer the following recommendations for those using version 6.0 or are unable to apply SP1 to 6.5.

There are a number of things that can be done to partially or wholly mitigate the risk posed by this vulnerability. The following are some examples. The reader is encouraged to understand their environment and business needs and base their solution around those.

- * Use or write an NSAPI module similar to the sample provided to inspect the length of HTTP request URIs. The module could be run as the very first NameTrans directive in the default object so that it will apply to all incoming requests. The sample allows a maximum length for the URI to be specified in the obj.conf file, will log an error if it is exceeded, and will send a "440 Possible Attack Detected" response to the client.

- * Terminate the SSL session on a device before the Sun ONE web server and install an IDS sensor to monitor the clear-text traffic. Write a filter to detect abnormally long HTTP request URIs.

- * Terminate the SSL session on a reverse-proxy that performs data validation on all HTTP request headers. If a specified length is exceeded or a pattern matches, log, alert, and send a warning down to the client.

```
=====  
NSAPI Data Validation Module:  
=====
```

Usage:

In `[server-root]/[server-instance]/config/obj.conf`:

...

```
Init fn="load-modules" shlib="[path to libs]/long.so"
```

Securiteam: [NT] Sun ONE (iPlanet) Application Server Connector Module Overflow

```
funcs="bounds_check"
```

```
<Object name=default>
```

```
# Make sure this function is the first to be called
```

```
NameTrans fn=bounds_check maxlength=500
```

```
...
```

```
----- BEGIN -----
```

```
#include "nsapi.h"
```

```
static int max_req_len = 0;
```

```
NSAPI_PUBLIC int bounds_check(pblock *pb, Session *sn,
```

```
Request *rq) {
```

```
char *temp;
```

```
max_req_len = atoi(pblock_findval("maxlength", pb));
```

```
temp = pblock_findval("uri", rq->reqpb);
```

```
if (temp != NULL) {
```

```
if (strlen(temp) > max_req_len) {
```

```
log_error(LOG_SECURITY, "bounds_check", sn, rq,  
"Overly long URI header (%d bytes)...
```

```
aborting.",
```

```
strlen(temp));
```

```
protocol_status(sn, rq, 440, "Potential Attack  
Detected");
```

```
return REQ_ABORTED;
```

```
}
```

```
}
```

```
return REQ_NOACTION;
```

```
}
```

```
----- END -----
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:advisories@atstake.com>>

@stake Advisories, <<mailto:kdunn@atstake.com>> Kevin Dunn,

<<mailto:ceng@atstake.com>> Chris Eng.

```
=====
```

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

```
=====
```

```
=====
```

Securiteam: [NT] Sun ONE (iPlanet) Application Server Connector Module Overflow

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, consequential, loss of business profits or special damages.