

[NEWS] Python Arbitrary Code Execution Through SimpleXMLRPCServer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0066.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/17/05

To: list@securiteam.com

Date: 17 Feb 2005 16:49:38 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

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

Python Arbitrary Code Execution Through SimpleXMLRPCServer

SUMMARY

Python is "an interpreted, interactive, object-oriented programming language. Python combines remarkable power with very clear syntax. It has modules, classes, exceptions, very high level dynamic data types, and dynamic typing. There are interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac, MFC). New built-in modules are easily written in C or C++. Python is also usable as an extension language for applications that need a programmable interface".

A vulnerability in the way SimpleXMLRPCServer has implemented its register_instance() function allows remote attacker to read and/or modify global values used by the Python program.

DETAILS

Vulnerable Systems:

* dev-lang/python version 2.3.4 and prior

Immune Systems:

Securiteam: [NEWS] Python Arbitrary Code Execution Through SimpleXMLRPCServer

* dev-lang/python version 2.2.3-r6 or newer

Description

Graham Dumpleton discovered that XML-RPC servers making use of the SimpleXMLRPCServer library, which utilizes the register_instance() method to register an object without a _dispatch() method, are vulnerable to a flaw allowing to read or modify globals of the associated module.

A remote attacker may be able to exploit the flaw in such XML-RPC servers to execute arbitrary code on the server host with the rights of the XML-RPC server.

Solution

Python users that don't make use of any SimpleXMLRPCServer-based XML-RPC servers, or making use of servers using only the register_function() method are not affected.

It is highly recommended to upgrade to a newer version as well.

ADDITIONAL INFORMATION

The information has been provided by <mailto:koon@gentoo.org> Thierry Carrez.

Python PSF-2005-001 <<http://www.python.org/security/PSF-2005-001/>>
<http://www.python.org/security/PSF-2005-001/>

=====

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

=====
=====

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.