

[NEWS] PeopleSoft XML External Entities Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0057.html>

From: support@securiteam.com

Date: 01/22/03

From: support@securiteam.com

To: list@securiteam.com

Date: 22 Jan 2003 21:24:56 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

PeopleSoft XML External Entities Vulnerability

SUMMARY

ISS X-Force has discovered a flaw in the PeopleSoft Application Messaging Gateway. PeopleSoft enterprise software enables the management of all manner of business functions, including human resources, customer relations, supply chain, and finance. The PeopleSoft Application Messaging Gateway provides a Web-based interface for PeopleSoft functionality and allows for communication and synchronization between PeopleSoft products non-PeopleSoft products.

DETAILS

Affected Versions:

PeopleTools 8.1x prior to 8.19, included with most PeopleSoft installations, including but not limited to:

- * PeopleSoft HCM (Human Capital Management)
- * PeopleSoft CRM (Customer Relationship Management)
- * PeopleSoft EPM (Enterprise Performance Management)
- * PeopleSoft FMS (Financial Management Solutions)
- * PeopleSoft SCM (Supply Chain Management)
- * PeopleSoft ESA (Enterprise Server Automation)

Securiteam: [NEWS] PeopleSoft XML External Entities Vulnerability

* PeopleSoft SRM (Supplier Relationship Management)

Note: PeopleTools 8.4x is not vulnerable.

Impact:

The Application Messaging Gateway is configured to run by default on the PeopleSoft Web server, and is accessible as a Java servlet. Attackers can use an XML External Entities (XXE) attack to read any file on the vulnerable PeopleSoft application server under the security context of the Web server process. This attack may lead to the exposure of confidential information stored in vulnerable PeopleSoft installations.

Details:

The Application Messaging Gateway can be administered via the Gateway Administration servlet, accessible to all by default. This servlet can easily be disabled, but most administrators do not regard it as a security risk. The servlet can be used to add handlers, to which data sent to the gateway is delivered. PeopleSoft includes a handler to push data out of the PeopleSoft system, called the SimpleFileHandler.

Once this handler has been added via the gateway administration servlet, XML data can be submitted via an HTTP POST request. When responding to a request, certain elements of the data submitted are selected using an XML parser, and several XML tags are returned to the remote user within the response.

It is possible to include an XML external entity within those fields, which causes the XML parser to read arbitrary files. Data is returned to the remote user within the response. It is also possible to cause the vulnerable servlet to open arbitrary TCP connections.

Recommendations:

ISS X-Force recommends that all PeopleSoft administrators block or restrict access to the servlets in question. X-Force also recommends that administrators take advantage of the security mechanisms that BEA WebLogic Servers provide to restrict access based on the requirements of users.

Administrators should examine the following configuration properties and tune them to their individual environments. To address the issues described in this advisory, the following servlets should be restricted within the "weblogic.properties" file:

```
weblogic.httpd.register.servlets/gateway.administration=psft.pt8.config.ConfigServlet
weblogic.allow.execute.weblogic.servlet.servlets/gateway.administration=system
weblogic.httpd.register.servlets/gateway.handlers=psft.pt8.reader.ReaderServlet
weblogic.allow.execute.weblogic.servlet.servlets/gateway.handlers=system
weblogic.httpd.register.servlets/gateway=psft.pt8.gateway.GatewayServlet
weblogic.allow.execute.weblogic.servlet.servlets/gateway=system
```

PeopleSoft has addressed all of the issues described in this advisory in PeopleTools 8.19, available on PeopleSoft's Customer Connection site in

Securiteam: [NEWS] PeopleSoft XML External Entities Vulnerability

early February. As a workaround, in addition to recommendations mentioned above, remove the SimpleFileHandler files if SimpleFileHandler is not required by deleting the /psft/pt8/filehandler directory under the servlets directory on the Web server.

Vendor Notification Schedule:

Initial vendor notification: 11/11/2002

Initial vendor confirmation: 11/11/2002

Final release schedule confirmation: 1/20/2003

ADDITIONAL INFORMATION

The complete advisory can be downloaded form:

<<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21811>>

<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21811>

The information has been provided by <<mailto:xforce@iss.net>> X-Force.

=====

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.