CERT/CC Blog

Vulnerability Insights

The Risks of Microsoft Exchange Features that Use Oracle Outside In

POSTED ON JUNE 4, 2013 BY WILL DORMANN [/AUTHOR/WILL-DORMANN] IN VULNERABILITY ANALYSIS [HTTPS://INSIGHTS.SEI.CMU.EDU/CERT/VULNERABILITY-ANALYSIS/]

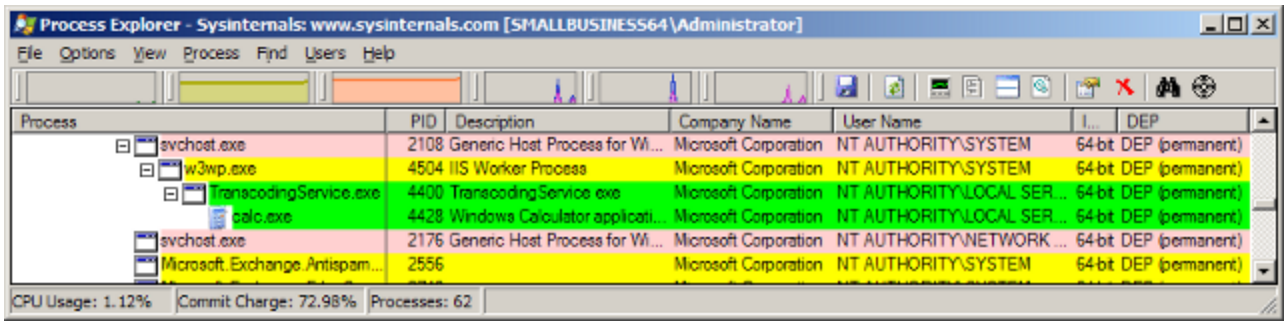
The WebReady and Data Loss Prevention (DLP) features in Microsoft Exchange greatly increase the attack surface of an Exchange server. Specifically, Exchange running on Windows Server 2003 is particularly easy to exploit.

It's public knowledge that Microsoft Exchange uses Oracle Outside In [http://technet.microsoft.com/en-us/library/dd351225%28v=exchg.150%29.aspx]. WebReady [http://blogs.technet.com/b/exchange/archive/2007/03/23/3401668.aspx], which was introduced with Exchange 2007, provides document previews through the use of the Oracle Outside In library. Outside In can decode over 500 different file formats and has a history of multiple vulnerabilities. See CERT vulnerability notes VU#520721 [http://www.kb.cert.org/vuls/id/520721], VU#103425 [http://www.kb.cert.org/vuls/id/103425], VU#738961 [http://www.kb.cert.org/vuls/id/738961], and VU#118913 [https://www.kb.cert.org/vuls/id/118913].

In the past, Microsoft Exchange provided only a subset of the file format parsers provided by Outside In, in particular, only the parsers required to process the file formats that are explicitly supported by WebReady. This limited distribution restricted an attacker to finding vulnerabilities in that subset of parsers. However, the currently supported versions of Microsoft Exchange provide the **entire** set of parsers provided by Outside In. This full distribution greatly increases the attack surface of Microsoft Exchange.

As part of the development of the CERT FOE [http://www.cert.org/vuls/discovery/foe.html] and BFF [http://www.cert.org/vuls/discovery/bff.html] fuzzing frameworks, I tested the latest versions of Outside In available from Oracle. Within approximately 5 minutes of fuzzing, I had a test case that demonstrated full control of the instruction pointer. I confirmed that a crashing test case from the Outside In fuzzing

campaign can be used to achieve code execution on an Exchange server by way of WebReady. The minimization-to-string feature [http://www.cert.org/blogs/certcc/2012/04/cert_basic_fuzzing_framework_v.html] in FOE and BFF made it pretty straightforward to make a PoC.



Exchange 2013 also uses Outside In for DLP [http://technet.microsoft.com/en-us/library/jj150527%28v=exchg.150%29.aspx]. If Exchange 2013's DLP is configured to scan attachments, then simply sending a message that has a malformed attachment through the Exchange server could trigger a vulnerability in Outside In.

So what do we do about this mess? Luckily, there are a few options:

Disable WebReady

The most effective way to mitigate Outside In vulnerabilities in Exchange is to disable the WebReady Document Viewing feature. Details of how to do so are available in the Microsoft Exchange Team Blog [http://blogs.technet.com/b/exchange/archive/2007/03/23/3401668.aspx], in particular, un-check the "Enable WebReady Document Viewing" option.

Use a Platform that Supports ASLR

If you can't disable WebReady in your environment, make sure that every instance of Microsoft Exchange is running on a platform that supports ASLR, in other words, Microsoft Windows Server 2008 or later. Microsoft Windows Server 2003 does not support ASLR and is therefore an unsafe platform to use with Microsoft Exchange WebReady. The above screenshot was taken on a Windows 2003 Server system running Microsoft Exchange 2007. See the Microsoft SRD blog entry On the effectiveness of DEP and ASLR [http://blogs.technet.com/b/srd/archive/2010/12/08/on-the-effectiveness-of-dep-and-aslr.aspx] for more details.

What About Microsoft EMET?

Microsoft EMET [http://www.microsoft.com/en-us/download/details.aspx?id=41138] can help to prevent the exploitation of many vulnerabilities. When this blog entry was originally crafted, I listed EMET as a mitigation against Outside In vulnerabilities in Microsoft Exchange. However, upon further investigation I have determined that EMET is not a viable solution on Windows Server 2003 x64. The reason is that despite what the EMET 4.0 beta documentation says, and despite what the EMET GUI may indicate, EMET does not yet provide ROP mitigations for 64-bit processes. I have received confirmation from Microsoft that this is the case.

Without the ROP mitigations, the added protection provided by EMET is severely limited. On platforms that do no support ASLR, attackers should be able to write exploits that function even with EMET protecting the application. If you are running Microsoft Exchange 2007 on a Windows Server 2003 system and you cannot disable WebReady, then you can add a small amount of protection by enabling EMET for the process that performs the WebReady conversion:

```
C:\Program Files\Microsoft\Exchange Server\ClientAccess\Owa\Bin\
DocumentViewing\TranscodingService.exe
```

As with any application that you choose to explicitly protect with EMET, it is important to verify that the software behaves as expected with the settings that you select.

Conclusion

If you are running Microsoft Exchange 2007 on a Windows Server 2003 system, you really should consider updating to a more modern platform that supports ASLR. While Microsoft Exchange 2010 and 2013 both use Oracle Outside In for the WebReady feature, those versions run only on platforms with ASLR, which makes exploitation difficult. The same is the case for Exchange 2013's DLP functionality. It is only available on platforms that support ASLR. We are currently working with both Oracle and Microsoft to help them improve the security of their products.

About the Author

Will Dormann

Contact Will Dormann [https://www.sei.cmu.edu/contact.cfm]
Visit the SEI Digital Library for other publications by Will [https://resources.sei.cmu.edu/library/author.cfm?authorID=2547]
View other blog posts by Will Dormann [/author/will-dormann]