

The Deep Queue

WebSphere MQ Security Podcast Episode #5, November 28th, 2008



Welcome to The Deep Queue for November 29th, 2008. For those of you in the USA, I hope you have a happy Thanksgiving. For everyone else, Thanksgiving is a holiday we have here in the states where we have a feast and then teach our children about sports betting. The Dallas Cowboys won last night and my son is giving thanks he only bet me \$10. I hate taking money from the kid but it's for his own good and it *is* an American tradition.

Some quick podcast news. I've heard back that the sound quality was low and had too much dynamic range. I'm using vocal compression and normalizing the volume for this episode and am hoping it will sound a little better. Please let me know what you think. I'm also providing a transcript at the request of a listener who explained that, as a non-native English speaker it was difficult for him to follow the show in the kind of noisy environment where he normally listens to podcasts – his daily train commute. Hopefully this will solve that problem. I'm trying out IBM ViaVoice software for the transcription and it does seem to get a very good percentage of the words but it doesn't catch the punctuation, paragraph breaks and so forth so I still need to spend a fair amount of time editing. You can add these in while dictating but if your primary output format is audio you don't want the show filled up with voice commands to format text. Upshot of all this is that transcripts would seem to limit the frequency of the podcasts. I had originally said I might go to twice a month or even once a week if the podcast was successful, but I think it's more important to provide the transcripts than to have lots of episodes.

We now also have an iTunes feed. The address is posted on the web site. I will be real curious to see how many folks subscribe through iTunes vs FeedBurner. I don't particularly dislike iTunes but never installed it since I don't have an iPod. Now that I have and set up an iTunes feed, the first thing I noticed is that it's very graphical and now I need a logo for the show. If there's one thing I really stink at that would be visual design so don't expect much in the logo department. Of course all you Apple aficionados are probably all graphic design wizards so if it really bugs you, feel free to whip something up and email it to me.

Oh yeah, one last piece of podcast news, is that starting with this episode, all of the links related to the show are now posted on Delicious as well as with the show notes. There will be a category per episode to keep all the links for each show together. Between shows I'll post interesting links with a WMQ security tag so you can subscribe to that if you want to see the whole stream as it happens.

I have to mention the conference in Barcelona. It was one of the best I've been to in a few years. This was the combined Transaction & Messaging and WebSphere Technical conferences. It is still more technically focused than IMPACT but diverse enough to draw quite a large crowd. I really enjoyed the city and the people and wish I had more time to get out and sightsee. I was able to meet many of my friends from the list server in person for the first time and made a number of new friends. This is for me the best part of the conference. It's one thing to meet people on an engagement where there are pressures from an outage or some urgent project and quite another to talk in a relaxed setting.

The new Advanced Security presentation debuted at the conference and was well received, which was a relief to me. If you have not had a chance to see it, you can download it from my web site. Any feedback is always appreciated. The presentation is an overview of design considerations when creating a WMQ security model. There is some discussion of the different classes of user and the access they require, asset isolation, defense in depth, how network topologies impact security, and more. The presentation is pretty abstract and I wanted to balance that out with some specific configuration advice so I distilled a bunch of hardening info down to bare bullet points. The list of bullet points alone takes up 13 slides. It should be a good starting point for anything from building an application security model to hardening a gateway. If nothing else, 13 pages of bullet points gives you something to show management to show why WMQ security is not trivial.

I'll be presenting the Advanced WMQ Security session at the internal conference for IBM Software Services folks and hope to present it at IMPACT this year as well. I submitted the proposal to the IMPACT selection committee and am waiting to hear back. If you have something to present at IMPACT, the Call for Speakers is out and you have until January 16th to respond. Last year A.J. Aronoff from Prolifics presented a session called *WMQ Enterprise Security: A Series of Defenses to Withstand the Test of Time* and we cross-promoted our sessions. If you are going to submit a presentation that talks about some aspect of WMQ security, feel free to contact me if you want an extra pair of eyes on it before it goes to the selection committee. I'm not on the committee and not involved in the selection but I want to encourage development of new WMQ security content as much as possible. And if your presentation displaces mine at the conference, I'd take that as a sign of success. It would mean that other people are getting really good at this stuff and it would indicate wider industry acceptance of the need for better security in the middleware layer. So start making plans to come to IMPACT and I'll look for you there.

OK, it's time for WMQ Security News and the news this month is all good. A new friend I met at the conference told me about the WMQ port scanner available from Roger over at Capitalware.biz. According to the web site, "MQPortScan will scan a range of ports for a given server looking for a queue manager's Message Channel Agent, using the standard (system default) channel names, in order to make a successful connection." One of the things that I see a lot is people will use non-standard WMQ ports in the name of security. That makes about as much sense as building your house with the front door moved over to one side in an effort to deter burglars. As this tool demonstrates nicely, security by obscurity barely even qualifies as a speed bump on the information highway. Chances are it has more of an impact to your organization than it ever would to an attacker.

When I had this conversation recently with a client the guy said "well, at least it makes the auditors happy." So I asked him "you implemented a "solution" which gives the perception of improved security without actually improving security...how is this a good thing exactly?" To my way of thinking, it is a bad thing when the perception of security exceeds the actual security. Anything that tips the balance toward heightened perception without a corresponding and measurable actual improvement just increases risk. This is because that nice warm fuzzy safe feeling makes it a lot less likely that resources needed to make a real difference are ever going to be allocated. If the goal is simply to get past the audit, congratulations you did it. If the goal is to reduce the likelihood of a successful attack or minimize the impact of such an attack switching to a non-standard port – switching ports doesn't get you any closer to that goal.

So, why do I like the Capitalware Port Scanner tool? For a few reasons, the first of which is that it lets us move past playing the shell game with ports and on to more effective counter measures. But a more subtle and perhaps more important benefit is that such tools mean that many more people will be

testing and probing their messaging networks looking for vulnerabilities. One of the reasons that WMQ security has languished on the back burner of so many shops is the lack of tools for security scanning and baseline compliance. Off-the-shelf tools lower the barriers in terms of knowledge and resource requirements necessary to perform scans and they tend to provide more consistent and reliable results than if each shop has to create their own tools from scratch.

Of course we need to keep in mind that security tools are a double-edged sword and they can be dangerous! Although I would encourage everyone to use the tools that are out there to scan their network, it is absolutely essential to get permission first! Last week on the Security Now podcast, Steve Gibson reported yet another story about a well meaning sysadmin who got fired. The company in question had a server with lots of confidential information and they put it out front of the building with the trash. The guy picked up the server and ran SpinRite on it which revived it. He then booted it up in front of the guys who had sworn up and down it was dead. The executives got wind of this and instead of thanking the guy for saving their bacon, they said he had misappropriated the sensitive data and canned him. The issue here, as it applies to us testing the messaging network, is that once you have gained administrative access it is impossible to prove that you did NOT copy off sensitive data. However it is usually possible to prove that you had your hands in the cookie jar because you are going to leave traces somewhere. Forget about “reasonable doubt” here because the standard used in civil cases, at least here in the USA, is a *preponderance* of evidence. The impossibility of proving a negative – that you did not steal or copy anything – weighed against the wealth of evidence you are sure to leave behind is the textbook illustration of what “preponderance of evidence” means. So no matter how pure your intentions are, if you perform an unauthorized security test you are just asking for trouble. By all means do the test, just get buy-in from your management first.

Also in the news for this episode, there are two new CVEs for WebSphere MQ. “CVE” stands for “Common Vulnerabilities and Exposures”. According to the web site (which we have a link to on the show's blog entry) “CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this 'common enumeration.’” In other words, each new and unique vulnerability that is discovered is given a number so that different vendors can refer to it by the same name. For example, if a new virus is discovered in the wild and you want to know if your anti-virus vendor has patched it, you can refer to it by the CVE number and find out. Even in the case of something like WebSphere MQ where there is only one vendor involved, the CVE system helps by providing a common reporting framework that all the independent security research teams can report into. If two teams find the same vulnerability, the reports are unduplicated and only a single CVE number is assigned. This was the case when both National Australia Bank and MWR Infosecurity independently discovered and reported the same WebSphere MQ channel vulnerability which became CVE-2008-1130. I've written a lot about that CVE but today there are four more I want to discuss and that will get us completely caught up on WMQ CVEs.

The first of these I wrote about on my blog and commented on how vague it is. CVE-2007-6044 is rated with a high severity specifically because it is so vague. I think the idea is to assume a vulnerability is severe by default unless proven otherwise. The description from the web site reads as follows:

Multiple unspecified vulnerabilities in IBM WebSphere MQ 6.0 have unknown impact and remote attack vectors involving "memory corruption." NOTE: as of 20071116, the only

disclosure is a vague pre-advisory with no actionable information. However, since it is from a well-known researcher, it is being assigned a CVE identifier for tracking purposes.

I have had discussions with one security researcher who reported memory a corruption vulnerability in WMQ and tells me that it has since been fixed. Because the CVE is so vague, we can only assume it refers to the same vulnerability. Entries like this in my opinion dilute the value of the CVE service but they seem to be the exception rather than the rule. My only advice here is that you would want to be on a Fix Pack that is at or above 6.0.2.3 anyway because of the channel vulnerability. This CVE dates back to 2007 (you can tell that from the name, by the way) and so should be included in any of the more recent Fix Packs.

CVE-2008-1592 is specific to Tandem and HP NonStop systems. These are a different code base than the distributed WMQ code and currently is at version 5.3. As of March 2008 when this CVE was published, WMQ did not enforce a requirement to be in the mqm group in order to use runmqsc. I will try to find out if this has been fixed but in the meantime, Fix Pack 5.3.1.4 was released just last month and if you are running on Tandem or HP NonStop, be thinking about upgrading to that. Especially if you use WMQ clusters because one of the fixes addresses a cluster cache corruption problem.

There are two more CVEs that are not publicly listed yet but have had candidate numbers assigned. Martyn Rucks of MWR Infosecurity gave a presentation at their "Making Sense of Risk" event on October 14th. In the presentation he discloses CVE-2008-4288 and 4289 for the first time, both of which are remotely exploitable denial of service attacks. He does say that these have both been patched although there is nothing obvious in the v6.0 fix list for these. You can download the presentation yourself from the MWR Infosecurity page and I have a little more news about them later on in the show.

My last bit of security news is about APAR IC56408 which is one that I reported. One of the issues that I've written about several times is that there are so few shops practicing WMQ security that the standards and best practices are still emerging. Many of the security features in WMQ have simply not been used that much or not at all. Every now and then when we start to use something it turns out that thing is broken. So as the community moves forward and adopts new practices, we inevitably uncover new issues. This APAR is an example of that phenomenon. I have always advised my clients to monitor for security related events. An example of this might include changes in membership of the mqm group. Obviously, WebSphere MQ authorization events fall into this category as well. What I found out was that on Windows platforms with Authorization Events enabled, it was possible to get a 2035 error that did not generate an event. There was a really nice error log message but if you are using something that monitors the event queues this doesn't really help you. Someone could launch a dictionary attack throwing 100 connection attempts a second at you and each with a different user ID and you would be blissfully unaware.

This would be a bit of a disappointment if you went to the trouble of restricting admin access, setting up application and user profiles, buying or writing something to watch for event messages and then enabling authorization events only to find that WMQ didn't bother to produce any! So if you happen to be in that group, and at least a couple of my clients are, you will want to upgrade to 6.0.2.5. If you are on v7 already, the fix is scheduled for 7.0.0.1 which the Fix Packs site shows as scheduled for the first quarter of 2009.

Well, that wraps the WMQ Security News for this episode. After the break I have an oddball assortment of stuff for a segment I'm calling, appropriately enough, "Random MQ Stuff".

BREAK

Welcome back. This is the segment I'm calling "Random MQ Stuff". It's all the odd bits and pieces I've been saving up that didn't quite warrant a full length article or show topic. I said earlier that I had some news about MWR Infosecurity and that's my first bit of "stuff".

As you may know from the blog or past episodes, I've collaborated with Martyn Rucks on some of his WMQ research from time to time and I have kept links to the MWR Infosecurity site on my page. Problem has been that their web site has not been set up to well to receive inbound links. I hate to link to someone else's PDF directly because I feel it is better etiquette to link to their web page so the reader sees the paper in the context that the author intended. But when I tried to link to MWR Infosecurity's WMQ whitepaper or their MQ Jumping tools, they were buried in a long page with no HTML anchors I could link to. It was very hard for readers to find these assets. Eventually I linked to the documents themselves and ran into a second problem – the links would break.

I told Martyn about the problems I was having and how it made it difficult for me to drive any traffic to their web site. That was a few months back and when I went to get links for this episode I noticed that they have a new "Labs" site at <http://labs.mwrinfosecurity.com> where they publish presentations, whitepapers, advisories and tools. This was a major enhancement to their web site and a very welcome addition for me because now I have a place to link to where people will have a better chance of finding the content and, hopefully, the links will be more stable. It is also the first time, at least as far as I know, that an independent security research team has provided a web site dedicated to reporting security research and vulnerabilities specific to WebSphere MQ. If you want to check it out, links are on my web site.

Random MQ Stuff Item number two – securing WMQ Extended Security Edition. Yes, you heard that right, you have to secure WMQ ESE. Like the base product, WMQ ESE is not secure if you leave all the default settings in place. It is necessary to do all the same administrative hardening when using ESE that you would do without ESE. In order to explain why, you need to understand how WMQ ESE works. When applications are locally connected, ESE intercepts API calls and applies authorization and protection policies. When the application is remote and using a client connection, the calls can be intercepted at the remote node or using a channel exit. There are two issues. First, the interception of calls only happens for application queues. Interception does NOT happen for calls against `SYSTEMADMIN.COMMAND.QUEUE` and you cannot enforce policy against this queue. This means that locally connected processes must be authorized at the queue level with `setmqaut` commands just like any other WMQ setup. The second issue is that ESE does not propagate the authenticated user ID into the `MCAUSER` of a client channel. This is not an issue when accessing application queues because the ESE object policy controls both the access and the resolved identity. But the user can still assert any identity on the connection and since ESE does not intercept calls to `S.A.C.Q`, the user can obtain full administrative rights if the channel is left exposed.

While this may be surprising, there is nothing particularly challenging about fixing it. The administrative hardening required for base WebSphere MQ installs works equally well with ESE installed. You set `MCAUSER` on the channel statically or with an exit. The only wrinkle here is that the ESE channel exit doesn't set the `MCAUSER` so you have to statically set it if you need the ESE channel exit. The couple of ESE installations that I've seen so far have not addressed this issue. That

means the security they've implemented in these cases only applies to application queues and it would be possible for an attacker to disable ESE. Unfortunately, this is a very limited sample and I don't yet have a good idea if this represents the ESE installations as a whole or if these are isolated cases. If you are running WebSphere MQ Extended Security Edition I would be very interested in hearing from you. Obviously I can't perform a free security assessment but I would be willing to exchange a few emails or even look at your saveqmgr output to see if these issues are addressed or not. If they are not addressed, you could use the instructions in the Basic WMQ Security presentation to fix the problem yourself or we could proceed with a formal assessment. I don't intend for this podcast to be a sales vehicle but if you have gone to the expense and trouble to buy and install WMQ ESE I am going to assume that you would not want to leave it running wide open and might need some help to remediate it in a timely fashion. Just be aware that help is available and I'll leave it at that. If this turns out to be a widespread issue, I'll expand this into a full article on developerWorks.

Random MQ Stuff Item number three – Availability. The goals of security support three basic requirements: confidentiality, integrity and availability. When it comes to availability most of the focus is on preventing or defending against denial of service attacks. But in the case of WebSphere MQ, there are as yet no publicly reported malicious attacks. What we do have plenty of though are accidental DOS attacks. One that I have seen repeatedly over the years is related to HA hardware clusters. One of my clients recently shot themselves in the foot with this one and reminded me to bring it up here.

The gist of the problem is that an HA cluster is one or more logical servers implemented on two or more physical servers. When an administrator signs onto the box the IP address or DNS name they use either is that of the physical server or it resolves to the physical server. Once signed on, it is not obvious whether the logical server is currently assigned to the same node. It may not even be obvious that the server in question is in fact participating in a hardware cluster. If the logical server is running on another node, it will appear locally that the queue manager is simply down. Attempts to start the queue manager will fail and if it is diagnosed and repairs attempted as if it were a stand-alone box, things can go downhill rather quickly.

The client I mentioned had just such an incident and when he was unsuccessful in starting the queue manager, proceeded to attempt to delete and redefine it. When that did not work, he manually removed the queue manager from the qm.ini file and tried again to define it. Eventually someone figured out that the QMgr was on another node in the hardware cluster but by then the configuration on the backup node was pretty badly mangled.

I have a couple of recommendations for this problem. The first is to make it obvious that the node is in fact part of an HA cluster. One way that I do this is to display a big sign-on banner telling the user "hey, this server is part of an HA cluster!" If you want to get really fancy, use the cluster management tools to display the current assignments of the resource groups. Of course the user only sees this once and if there are a lot of sessions open it may not be obvious later on which is which. So the other thing I do is to set up the prompt so that it is different on HA clusters than on stand-alone servers. This way the user has a continuous visible indicator which servers are stand-alone and which are HA.

One really important aspect of all this is to implement it in such a way that it is sustainable. Specifically, I like to only ever maintain one copy of the mqm user's .profile and make it work on all platforms. So the profile tests to see if the node is HA or not and then tailors the user's session accordingly. At my previous employer we had Solaris, HP-UX, AIX and Linux servers and all of these used the same .profile. If the user home space is on a shared drive, you almost have to do it that way.

If the users have local home space on each server the best solution I've found is a tool that automatically pushes new versions of .profile and other artifacts out to the mqm user's home space. The other thing I'll mention here is that the mqm user's home space should be treated like any other Production asset and subject to strict change control. You don't want to be editing the .profile file live and you will want to make sure it is thoroughly tested before pushing it out. Even though it's a bit more work, I actually like it better when the user home space is local because it makes it easier to test changes in an isolated environment.

My last and best bit of WebSphere MQ Random Stuff is about File Transfer Edition. The product General Availability date is December 5th for electronic download and December 12th for media and documentation. As I record this podcast, I am literally hours away from leaving for the UK to participate in a WMQ FTE residency where we will be developing content for IBM Education Assistant showing how to use and configure WMQ FTE. Aside from being excited for personal reasons, I think it is significant that there are so many resources behind this product launch. There has been an extensive Beta program, there have been customer feedback sessions and conference presentations already and then there's this residency to produce a body of educational content intended to help people get up to speed quickly. I believe that FTE will launch with as much or more Education Assistant content than WebSphere MQ has so that represents a significant commitment.

If you are not familiar with IBM Education Assistant, it is an Infocenter but instead of containing product manuals like the Infocenter you are probably more familiar with, it contains instructional video and screen shots, presentations and whitepapers that focus on the practical aspects of configuration and usage and step you through a process in detail. The materials here tend to be very task oriented and are intended to supplement the manuals. There are versions for all of the IBM software brands as well as the servers so there should be something there for everyone. It's a great resource and if you are not familiar with it, I invite you to go and take a look. I've posted a link with the show notes.

Links for this episode:

Deep Queue iTunes feed

<http://itunes.apple.com/WebObjects/MZStore.woa/wa/viewPodcast?id=298285838>

IMPACT 2009

<http://www-01.ibm.com/software/websphere/events/impact2009/>

IMPACT 2009 Call for Speakers

<https://www-950.ibm.com/events/IBMImpact/impact2009EMS/>

WebSphere MQ Enterprise Security:

A Series of Defenses to Withstand the Test of Time

http://www.prolifics.com/demos/impact2008/MQSecurityStrategyImpact2008_rfs.pdf

MITRE CVE web site

<http://cve.mitre.org/cve/index.html>

US National Vulnerability Database

<http://nvd.nist.gov/>

wmqsecurity deepqueue:episode005 software security search reference computing vulnerabilities
vulnerability infosec hacking hack

Fix list for WMQ 5.3 on HP Non-Stop

<http://www-01.ibm.com/support/docview.wss?rs=171&uid=swg27009174>

Fix list for WMQ 6.0

<http://www-01.ibm.com/support/docview.wss?rs=171&uid=swg27007069>

MWR Infosecurity Events page

<http://www.mwrinfosecurity.com/events.php>

http://www.mwrinfosecurity.com/publications/mwri_middleware-threats-presentation_2008-10-14.pdf

MWR Infosecurity Labs

<http://labs.mwrinfosecurity.com/>

WebSphere MQ File Transfer Edition

<http://www-01.ibm.com/software/integration/wmq/filetransfer/>

WMQ FTE Availability

[http://www-01.ibm.com/common/ssi/cgi-](http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ca&infotype=an&appname=iSource&supplier=897&letternum=ENUS208-331)

[bin/ssialias?subtype=ca&infotype=an&appname=iSource&supplier=897&letternum=ENUS208-331](http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ca&infotype=an&appname=iSource&supplier=897&letternum=ENUS208-331)