SECURITY NOW!

Transcript of Episode #21

The Windows MetaFile (WMF) Vulnerability

Description: Leo and I discuss everything known about the first serious Windows security exploits of the New Year, caused by the Windows MetaFile (WMF) vulnerability. In our show's first guest appearance, we are joined by Ilfak Guilfanov, the developer of the wildly popular - and very necessary - temporary patch that was used by millions of users to secure Windows systems while the world waited for Microsoft to respond.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-021.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-021-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 21 for January 5, 2006: The WMF Vulnerability.

Via Skype today because we're going to do a little conference call: Steve Gibson joining us from Irvine; I'm in Northern California; and soon to join us, Ilfak Guilfanov. We're talking about the Windows MetaFile (WMF) vulnerability.

Steve, why don't you recap the story so far.

Steve Gibson: And I have to tell you, Leo, that with this new microphone, even Skype sounds pretty good.

Leo: You sound really good.

Steve: Hello.

Leo: With your PR-40, yeah.

Steve: Yup.

Leo: All right. Thanks to Bob Heil.

Steve: Okay. So the Windows Metafile vulnerability is something which came to light due to its exploitation. The good news is that people didn't - the people who figured this out did not go stealth with it. Although on the other hand, of course, we don't know how long this might have been used secretly before it came to light up public attention.

Leo: And that's an important point because we called this a "zero day vulnerability," in other words, the exploits emerged immediately. But in fact it was the exploits that introduced us to the vulnerability. It wasn't Microsoft that announced it; or was it? Or was it a security firm that announced it? Who first discovered it? Was it SANS Institute or...

Steve: The timing was so close, I don't know. Although certainly Microsoft did have a notice up on - I believe it was on the 27th. On Tuesday the 27th they put up a notice saying that they realized there was a problem. It was in active exploitation. And they then set about fixing it.

Leo: So we really don't know how long the exploits have been going on, frankly.

Steve: No, I mean, in fact, you know, there have been people, sort of the conspiracy theorist people, who wonder, you know, that the NSA or CIA or, you know, shadowy government bodies might not have access to our machines with, you know, knowledge or not of unknown and still undisclosed vulnerabilities. So...

Leo: Because this is like a backdoor. Not an intentional backdoor, but it's very - it gives you that functionality. It's essentially a backdoor into Windows that Microsoft didn't mean to put in there, but has been there as far as - as long as we can tell.

Steve: Actually, as we know, it's a backdoor that they did mean to put in there. This thing was designed in. It's not a mistake. It's always been there. And someone realized, hey, we can use this to run whatever code we want on users' computers.

Leo: It was done in a day, I guess - and we've talked about this before - when programmers assumed the benevolence of their users and so gave them capabilities, not assuming that their users would be malicious. But of course now all programmers are trained to assume that users are malicious and to make sure they don't include this kind of code.

Steve: It's a whole different mindset today.

Leo: When the vulnerability was discovered on Tuesday, Microsoft offered a kind of a rude fix for it, which was essentially to unregister a DLL. Turns out that wasn't a very good fix. And very quickly, a fellow named Ilfak Guilfanov stepped forward. Who is Ilfak?

Steve: Ilfak has actually been known within the developer community for quite a while. He's the lead developer for a company called DataRescue. He's largely responsible for an amazing disassembler called the IDA Disassembler, which is really highly useful for anyone who's trying to take a blob of code to which they do not have the source and figure out how it works. And so for people who are disassembling and reverse-engineering viruses and other kinds of malware, it's a very powerful tool for giving them a look into unknown code.

Leo: I wonder if he used his disassembler to figure out what the WMF interpreter was doing.

Steve: I have no doubt that he did. In fact, I will be, if I end up writing a patch for Windows 9x.

Leo: Interesting. Well, we're fortunate enough - he lives in Liège, Belgium, and it is after 10:00 o'clock at night there. But we are fortunate enough to be able to talk to Ilfak right now. So let's dial him in via Skype. Hello, Ilfak.

Ilfak Guilfanov: Hi.

Leo: Hi. This is Leo and...

Ilfak: This is Leo? Okay.

Leo: Yeah. And Steve is with us.

Steve: Hi, Ilfak.

Ilfak: Hi, Steve.

Leo: And we all are good. I'm so glad that you could join us for this.

Steve: Ilfak, the one thing that I've seen mixed issues about is whether this vulnerability is created by a buffer overrun bug in the Windows Metafile processing, or is it just taking advantage of a feature which is working correctly and has always been there.

Ilfak: It is the latter, the second. It's not a buffer overflow. It is something that is by design. So the design of these WMF files allows to specify a code sequence to be executed. And this code sequence is in the file itself, so anything can happen.

Leo: And Windows makes no check on what that arbitrary code is. It just allows you to execute any code at all. Does the code have the same privileges as the running user?

Ilfak: Yes.

Leo: Wow. So if you're running as administrator, that's where the issue occurs. If you were running as a limited user, would you have a problem?

Ilfak: Well, you will still have problems like, for example, this malicious code could destroy, could delete your files or do something bad to your data.

Leo: Anything you could do.

Ilfak: Yeah.

Leo: But of course when you're running as administrator that includes installing a trojan horse or other malware.

Ilfak: Yeah. Everything can be done to your computers, yeah.

Steve: So this means that this code, or this feature, rather, has always been there and that - I mean, like for 15 years, at least. And so suddenly someone realized, basically had an inspiration that they could use this longstanding feature working correctly in Windows in order to leverage attacks against users who opened images.

Ilfak: Yes. Or they just found it by chance by just looking on the code, at the specification of these WMF files. And they saw, okay, that's something we can do with - we can do anything with a computer if we feed it a specially crafted WMF file.

Leo: It's really amazing that this hole has existed for so long.

Ilfak: Yeah.

Leo: Do you think anybody knew about it before but was keeping a secret?

Ilfak: Well, I think that, since the feature existed since long ago, there were people knowing about it, but they were not looking at it as something to exploit. After all, this feature is there by design. So it has a - it can be used for good, not only for bad things.

Leo: Right, right.

Steve: What do you think Microsoft will do, then, with this patch, in order to eliminate this without breaking any applications that may have actually been using this in the way it was intended?

Ilfak: Oh, it's a very, very tough question. I wonder what Microsoft will do with this. I don't know. Really I don't know because the feature itself is a vulnerability.

Leo: So, Ilfak, what does your program do? Does it completely disable Windows Metafiles?

Ilfak: No. It doesn't disable the files. It just disables one single function in these files. It's the function that executes this arbitrary code.

Leo: So that's presumably something Microsoft could do.

Ilfak: Yeah.

Leo: I wonder if it would break a lot of software. Have you heard reports that your patch is causing problems for people?

Ilfak: Yes, there were some reports like an old printer does not print anymore, something like that. I heard about problems, printing-related problems. So there might be some broken applications.

Steve: Well, and in fact that was something that you expected and talked about early on when this began to spread, that is, when your patch began to be used last weekend, was that it was clear that this involved printer-related aspects of Windows Metafiles.

Ilfak: Yes. I put a warning on my blog, saying if you apply these patches, there might be some bad consequences like printing problems or something else. I cannot tell. I cannot tell, but there might be bad problems.

Leo: Ilfak, you fixed the problem for Windows 2000 and Windows XP. But as I understand it, the problem also exists for Windows 95, 98, and ME. Is that true?

Ilfak: Oh, there were different opinions about this. And I still don't know for sure if these systems are vulnerable or not. They use completely different code. XP and 98 systems are different in this. They use different ddi.dll library. So I just cannot tell if they are vulnerable or not. But most likely they are not.

Steve: Now, your vulnerability checker does say that the system - that, when run on a 98 system, that it may be vulnerable.

Ilfak: Then it may be. I just, you know, I don't have the computer with 98, and I cannot check myself.

Steve: Oh, okay.

Ilfak: That's, unfortunately, that's the...

Steve: What's interesting is that Microsoft has just reissued their standard policy page. They've moved the 9x and ME systems off of that, which were previously listed. And in the FAQ section, they're saying now that they don't consider this to be a critical vulnerability because they haven't found an explicit way that this vulnerability could be used. And presumably it means they're not going to be patching the 9x and ME systems.

Leo: And since no one knows if you're vulnerable, it's kind of a little bit scary.

Steve: What I've told people on my site is that, if Microsoft doesn't fix this, I will.

Leo: Ilfak, how did you come to know about this vulnerability, and how did you write the fix so quickly?

Ilfak: I learned about it, as everyone else, from the news that's on the Internet. And I thought that it was a really dangerous vulnerability this time because you just go somewhere and browse, and that's all.

Leo: Microsoft did a kind of a very broad patch, but recommended a very broad patch, which is just to unregister the DLL. Did you feel that that was inadequate and decide to do something better?

Ilfak: Well, since the problem itself is not in this unregistered DLL, I felt that it might not be enough in all cases. That's why I developed my patch.

Steve: Well, and you were, of course, completely correct. The shell image viewer DLL, which is the one that Microsoft was recommending be unregistered, it was sort of a quick workaround that Microsoft felt comfortable recommending early on. But it was even then well known that there were other ways you could get Windows to parse a file that turned out to be a Windows Metafile, even if it didn't have a WMF extension, because Microsoft's looking inside the header of the file. And it was, you know, clearly not a good recommendation, although it may have been all Microsoft could do at the time.

Leo: Right. Ilfak, how many people downloaded that file from your site before Hexblog was shut down?

Ilfak: That's a difficult question because my site went down, and I could not even check my logs.

Leo: Oh, my. So you don't know.

Ilfak: No, I don't know exactly.

Leo: Steve, you've had at least 200,000 visits to the page, yes?

Steve: Yes, we have. Actually, now we've crossed a quarter million.

Ilfak: Whoa.

Steve: Our Episode No. 20 show notes crossed a quarter million viewings earlier today. It's at 252,711. So, I mean, this has clearly been, I mean, I've been seeing more site traffic myself at GRC than, you know, than I've seen in a long time.

Leo: Yeah.

Steve: And interestingly, Tuesday was even busier than Monday, and Wednesday was busier than Tuesday. Today it's quieting down and slowing down a little bit. But it's really, I mean, as the word spread, the need for this has been, you know, really widespread.

Ilfak, did you expect that what has happened was going to happen, that there would just be this incredible demand for what you wrote just basically for yourself; right?

Ilfak: No, I didn't expect anything like that. I just looked at this as a technical problem. I wanted to solve it, like to protect my computer and to present it to others. And it's up to them if they want to use it. If they use it, if they don't want to use it, again, it's their choice. I respect it. But it turned out to be much bigger than I thought.

Leo: Well, at this point PC Magazine, eWEEK, Steve Gibson and many others have recommended the Ilfak Patch. And as far as I know, it's the only effective patch out there. You are updating it; it looks like you have updated it. You're now at version 1.4. Tell me about the updates. Do they change the functionality of the patch?

Ilfak: No, they don't change anything in the patch itself. So if the very first version of patch works for you, there is no need to install or reinstall anything. It works pretty well and is the same protection as in the first version. The first version or the last version will give you the same protection. The only difference is that the first versions were not compatible with all systems. And each new release was adding support for a new version of the operating system, like Windows 2000 or SP2 or something like that. That's the only difference between the releases.

Steve: Well, in fact, that was how you and I first communicated, was you and I worked to add Windows 2000 compatibility to your very first release.

Ilfak: Yeah, yeah, yeah, exactly.

Leo: Well, we want to thank you on behalf of the entire Internet community, Ilfak. Obviously what you've done is you jumped into the fray when Microsoft was unwilling to and, frankly, risked liability doing so. And I think it's very brave of you, and I think it's a really great contribution. So thank you very, very much. I've run it, and I know everybody else who's listening has.

Steve: Yes, thanks, Ilfak. And...

Ilfak: I am happy to be of any help.

Steve: Well, and certainly we now know that there are literally hundreds of websites that are distributing images, trying to take advantage of this exploit. And, you know, who knows how many computers your patch has actively helped prevent being taken over by whatever malware was being used by this exploit in order to move it into people's computers.

Ilfak: Oh, we don't know. But let's hope that we have protected as many computers as we could.

Leo: But of course that raises the issue that, if you were already infected, running Ilfak's patch isn't going to in any way remove any malware on your system. It's just going to prevent further infections. But your infection is still there.

Ilfak: Yeah.

Steve: Well, that - yeah. And of course it raises an interesting point. People keep asking, how do I know if I've been infected by this? And they misunderstand what the "this" is. The exploit is sort of, like, creates an open door that allows anything else to be carried into your computer. So it's not so much that you're being infected by this exploit as much as, you know, it's being used to install Lord only knows what into your machine.

Leo: And even if you close the barn door, the horse may well be gone. Ilfak, I know it's late in Liège. So we thank you so much for joining us.

Ilfak: Thank you, Steve. Thank you, Leo.

Leo: And once again, thank you for the great job you did.

Ilfak: Thank you.

Leo: Ilfak Guilfanov, take care. Goodnight.

Ilfak: Bye.

Leo: Great to talk to Ilfak. And I didn't want to scare him, but I did raise the issue. You know why Microsoft is slow to release these, of course, is the liability issues if the patch goes wrong or is perceived to go wrong by people.

Steve: Well, and it has happened before that they've come out with a security patch which has broken other things. They did one, in fact, that we've referred to in a prior podcast, where they messed up some aspect of segment size. I can't remember exactly what it was now. But, for example, it caused VPNs that corporations were using to suddenly break after the corporations deployed the patch. So, yeah, I mean, it's really understandable. Now, we should mention that, by the time anyone hears this, Microsoft's final real official patch for Windows and for this whole Windows Metafile vulnerability will be publicly available.

Leo: Let's talk about that because it leaked out earlier.

Steve: Right, it leaked out Tuesday night, actually.

Leo: And normally Microsoft waits till the second Tuesday of the month for their patch cycle. So you're saying on Thursday the 5th at what time they're going to release the official patch?

Steve: It's at 2:00 p.m. on the West, which of course is 5:00 p.m. Eastern.

Leo: Just about as we record this, in fact.

Steve: Right, a little bit after we're recording it, it'll be made available. And this will be the official patch. I was notified that it was available Tuesday. I quickly grabbed it. I took great pains, of course, to check the digital signature chain to make sure that this was, I mean, really, truly from Microsoft. And I verified that the root certificate that was anchoring the trust chain - of course we'll be talking about all of this stuff in podcasts very quickly, I mean, very soon here in 2006. I verified that it was the same root certificate that had signed other patches, official patches from Microsoft. So the only way for that to be true is if this file that I had downloaded from some file archiving site was truly signed by Microsoft.

Leo: Let me ask you, did you run the patch?

Steve: I did.

Leo: And did it fix the vulnerability? In other words, did the tester that Ilfak has written come up clean?

Steve: Yes, it fixed the vulnerability. And what was interesting, and what I wanted to verify for everyone, was that there wasn't any problem interaction between what Ilfak had done and what Microsoft has done.

Leo: Right.

Steve: And of course I did review the source code when I was working with Ilfak on this last weekend. So I knew that, I mean, I knew to expect no problem. And so my advice had been to go ahead and install Microsoft's patch when it's available, and then remove Ilfak's. See, what his does is actually it suppresses the vulnerability. It doesn't actually patch the files, as you and I talked about in our special edition of Episode 20 over the weekend; it just prevents this from happening without actually modifying, physically modifying the file. It makes some in-memory changes that just sort of kills that function that Ilfak was explaining is something deliberately that's always been part of Windows Metafile.

Leo: So his program loads on boot and runs in memory, blocks it; but Microsoft's will actually patch the - presumably will patch the underlying file. At which point you would want to uninstall Ilfak's patch. There's no reason to have that running in memory.

Steve: Correct. And the other thing that was really interesting is that Microsoft's file, the version of the new GDI32DLL, which is the single file that's changed, it was dated Wednesday evening of last week.

Leo: Hmm.

Steve: Meaning they really did jump on this immediately.

Leo: And were able to fix it.

Steve: Yes, as far...

Leo: It seems like it would be a simple thing to fix. You just, you know, you turn off that arbitrary code execution...

Steve: Well, I mean, and that really is the issue. And I don't yet know, and Ilfak doesn't know, I don't think anyone knows until we look at the code or until Microsoft formally states what it is they've done, I mean, they have actually had to turn off, perhaps turn off a feature which Windows Metafile processing has had from its inception.

Leo: And some GDI printers will expect, apparently.

Steve: Well, yes. Which is certainly a feature that's going to have some interaction. Now, I received a blurb - because I've been in the middle of all this here for the last week. Nothing else has been done over at GRC except, you know, dealing with this. And I may in fact find myself writing a patch for Windows 9x and ME users if Microsoft doesn't address it. And it looks like they're not planning to, which is distressing a lot of people.

Leo: Well, I think they're end-of-line on those products. They don't promise support.

Steve: Actually not.

Leo: No?

Steve: I checked that out, and they are officially supporting 98 and ME through June of 2006. They had originally said they were going to end it, I think sometime in 2004.

Leo: Right.

Steve: And there was such a hue and cry from people saying, hey, wait a minute, we're still using these things, and the code's buggy. We need you to keep it current. So they said, oh, okay, fine. And but so arguably they really should patch Windows 98, but apparently they have no plans to.

Leo: Well, we'll see. I mean, they may not do it today; they may do it later.

Steve: I heard a quote from someone - actually it was a press person who forwarded to me something from Microsoft's website. It was, I think, a PR person that he was speaking with, saying that as a consequence of this they're going to be reexamining other things like this. And he said, you know, what do you make of this, Steve? And so, you know, decoding it from, you know, PR speak, it sounded like exactly what Ilfak has said. And now this all sort of makes sense. It's they may have looked in the past at opportunities for buffer overruns, but this was not a buffer overrun. This was written in the days when nobody was thinking about security. No one was...

Leo: It made sense to write a feature that, if the file format is corrupted or fails, you're allowed a fallback routine. And it sounds like, if they did it in this, they may have done it in many, many other situations.

Steve: Well, and what's really interesting is that the image itself, or that is to say the Windows Metafile itself, contains the code which you can cause it to execute. So it was like, I mean, you know, it was literally like by design an image file would contain executable code.

Leo: Well, I guess - I'm just guessing, reading tea leaves, that the idea was that you would put some sort of fallback routine if the GDI calls weren't - I would imagine an issue was if the GDI calls weren't supported. Maybe there were various versions of GDI. And if a printer didn't support the calls necessary to render the image, then you could have a fallback routine in the image, something like that.

Steve: Yeah.

Leo: And I bet you that that's a technique that Microsoft has used widely, which means hackers are going to be looking for other areas to exploit. And there may be many.

Steve: Well, certainly with our current understanding of security, no one in their right mind would create a file format which contained, you know...

Leo: Executable code.

Steve: Literally, where you could put binary code in. Now, you know, there are, I mean, you know, people are having all kinds of problems with scripting. And I know that, you know, we've seen PDF files that have had problems. And PDFs are, you know, executable PostScript-style code. So, you know, these kinds of powerful technologies, you know, with the power comes security concerns.

Leo: One wonders if Adobe used a technique like that in the PDF file format for a failback routine.

Steve: Well, it couldn't have been binary executable because, of course, PDFs have always been cross-platform. They've been able to run...

Leo: And they're texts, they're interpreted texts, basically.

Steve: Exactly.

Leo: Yeah, yeah.

Steve: Whereas, in the case of a Windows Metafile, this was, you know, Intel binary code...

Leo: Right.

Steve: ...where something just said, oh, start running here.

Leo: Right.

Steve: And Lord knows.

Leo: Wow.

Steve: It's been an amazing week.

Leo: Well, Steve, I'm glad that we were able to cover this. I know it wasn't on our schedule. We were going to talk about other issues. But we'll come back next week. What will we talk about next week?

Steve: Next week we're going to talk about - we're going to lay some foundation for basic Internet technology, you know, what are packets, what is routing, what is the IP address space? We'll talk about IPv6 and what it means, sort of lay some foundations for a number of different things we want to be able to talk about in the future. So sort of like, you know, nail down some terminology.

Leo: Once again, barring any nasty exploits of any kind because, of course, we always cover those first. That's what this show is all about.

Steve: And for what it's worth, for people who are listening to this that have Windows 9x or ME, if it turns out that Microsoft is not going to fix this and there is a problem, and it seems to me that there is, I'll be coming up with some sort of a solution for it.

Leo: Stay tuned. We'll put a link in the show notes to Steve's site, talking about this vulnerability and offering Ilfak's patch. Although, again, by now you won't need it. You can run Windows Update, and Microsoft Windows will automatically be patched using an official Microsoft fix. They plan to ship it on January 5th at 5:00 o'clock Eastern, 5:00 p.m. Eastern. But again, you can go to GRC.com/sn/notes-020.htm, or I should say zero two zero dot htm, if you want to know more. Or just go to GRC.com and go to the show notes page, and you'll find a link there.

Now Heil-powered for your enjoyment. You ran out and got a PR-40, huh, Steve?

Steve: Yeah. Well, you sounded so good when you switched to yours, I thought, okay, I've got to have one as big as Leo's.

Leo: Steve, you should have asked me. I'm sure Bob Heil would have sent you one.

[Talking simultaneously]

Leo: He's a fan. All right. Well, thanks to Bob Heil for my PR-40, anyway. And of course to AOL Radio and the AOL Podcast Channel, where this show appears. And they provide us the bandwidth to make it possible to offer you Security Now! absolutely free, every single Thursday. Steve Gibson, we'll talk again next week, if not sooner.

Steve: Right-o.

Leo: Thanks for joining us.

Steve: Thanks, Leo.