Hello, I'm Roger Safian. Today is Thursday July 5th and you’re listening to the information security news podcast brought to you by Northwestern University Information Technology. It's going to be a short podcast this week. I think a combination of the 4th of July holiday here in the United States and these crazy temperatures that we've got here in Chicago have produced not a lot of news or at least not a lot of news that I’ve found. So, I’ve only got three stories this week.

The first one is another update to WordPress. So, if you've got a website and you're running WordPress on it, please make sure that you grab the latest version. That's 3.4.1 that's out there right now and you want to take care of making sure that you get that installed on your system, because WordPress, we've seen it in a fair number of incidents here on campus.

Then I want to talk about a tool that's put out, it's the PSI, which is the Personal Software Inspector. It’s put out by Secunia, and we've talked about this tool before and basically what it does is it goes through your machine, looks to see what programs you have and then looks to see if they’re up to date. And that's pretty good because while a lot of software, you know, say the Microsoft products or maybe the Adobe products now, you know a lot of different products are updating themselves automatically there's a lot of stuff that's not. So, it's pretty cool to be able to do this, though one thing that is sort of a concern I have about tools like this, is it only checks for the programs that it knows about. So, if you've got some program on your machine let's say you've got a game, if it doesn't know about that game it's not to be able to tell you if there's a newer version of it, you know and did that version have security holes or something like that. So, it's I guess am trying to say it's not the complete solution where it will check every single program on your computer and look to see if there are newer versions of them but does get the lion’s share of stuff. When I ran it on my machine I think it found like 90 different programs that it knew something about and all but 88 or something like that had already been updated. So, I'll put a link to it in the show notes. It's certainly worth doing and taking a run, you know, it doesn't hurt anything. It's always nice to look at your machine and make sure that you’ve got it.

And then the last official story I want to talk about, and then I want to have a rant about something for just a moment, is a story about Apple. It was four signs that Apple is sharpening its security game and we talked a little bit about this recently since the flashback incident where you know Apple is kind of changing the way that they're doing things. And here's another story that basically says that. And the four points that they give are that the Safari browser now disables unpatched Flash plug-ins, which is pretty cool. That Apple’s changed their Macs don't get viruses claim anymore on their websites, now it’s just that they’re just a secure machine. Apple you know the flashback incident itself you know they helped...
derail that. And then Mountain Lion is going to get automatic updates and that’s pretty cool and I really hope that it works out where it’s truly automatic updates. You know, I hate to see people given the opportunity to say no, because they will. I know we’ve talked to an awful lot of Macintosh users. It seems like lately the only virus problems we’re having are Macs and you know almost all of them that we’re speaking to now just don’t bother updating their machine. You know we’ve even asked them and some said “oh yeah I just ignore it” you know so really good thing that Mountain Lion is going to get this and I hope it’s truly automatic updates. My understanding from reading a little bit about is it’s supposed to once a day to check to see if there are updates out there. Which is pretty cool.

And then the last thing I want to talk about, a little bit of a rant, and that is there is a hole in Cisco’s WebEx player, and this is the WebEx player it’s, the hole’s there on Windows, Mac OS, Linux, you know, so vulnerability in just about everything. And Cisco does have a updated version of their WebEx client on their website so you can download and install and solve this error. But they make it very difficult to figure out exactly what it is that you’re supposed to do, which version of the WebEx player you’re supposed to download and there’s two different versions for both Windows for Mac, Linux, you know which one am I supposed to get? It’s, it’s, confusing as hell! Why didn’t they just put a little widget on their webpage that says “click here I’ll look at your machine, figure out what you got and update it for you” instead of trying to make you figure out what it is, because a lot of people are going to get this wrong. So, Cisco you’ve totally blew it on this here and here’s my advice if you’ve got a WebEx player on your machine right now, and you probably do if you’re using it for business purposes, go and uninstall the WebEx player. The next time you need to go to a WebEx it’ll automatically grab the latest version it’ll be the right version you won’t have to worry about trying to figure out which one it is. And then you’ll have it, but at least you won’t have this vulnerable version of the WebEx player sitting on your machine. And again I’ll put a note to this in the show notes, so that you can take a look at this if you like. But Cisco, you know you’ve really blew it on this one, sorry.

That’s all I want to talk about so thanks for listening. If you have any comments or suggestions please feel free to send them to r-safian@northwestern.edu and as always you’ll find additional security information as well as the notes that contain the links for today’s podcast at our website www.it.northwestern.edu/security.