

Microsoft IIS WebDAV Remote Authentication Bypass with Amichai Shulman

Listen to Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit [Imperva.com](https://imperva.com), check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Joining me today is Amichai Shulman, CTO and Co-founder of Imperva.

Welcome to the show, Amichai.

Amichai Shulman: Thank you Brian. It's great to be here today.

Brian Contos: So, Amichai this is sort of an impromptu podcast that we are doing today and this is because of the new Microsoft release IIS WebDAV Remote Authentication Bypass. It's quite a mouthful. For those of you who may have not heard of this yet it's been getting a lot of popularity the last couple of days. May 18th was the official publication date of the vulnerability by Microsoft. But I'm actually just going to read a short little paragraph verbatim here about what Microsoft says about this, just for a little background.

"The Microsoft IIS server is a web server that is included with the standard server versions of Microsoft Windows Operating System. The IIS Web server includes a WebDav or a web-based distributed authoring and versioning feature which allows clients to update files on the IIS web server. The products that are impacted are Microsoft IIS Web Server 5.0, 5.1 and 6.0. The vulnerability might allow a remote attacker to access protected files without a password. Successful exploitation of the vulnerability can result in the following: authentication bypass of password protected directories, manipulating files in the password protected WebDav directory."

So, quite a mouthful. We've seen a lot of vulnerabilities like this over the years, Amichai. What makes this one successful?

Amichai Shulman: To tell you the truth, Brian it's not. To me it's like the sequel of a bad horror movie.

Because if you take a look at the components of this vulnerability basically what we have here is an UTF-8 encoding vulnerability in WebDav service. Now, I think that since the beginning of WebDav support in IIS servers there is very small percentage of actual deployment using this feature, especially in web facing applications. And I think that the first recommendation for anyone using IIS would be turn off WebDav support.

So, it's amazing to me that by now there are so many servers out there still affected by this vulnerability. I think I saw some statistics saying that 90 percent of installed IIS servers still have WebDav enabled. And then UTF-8, we had it like three or four years ago. And by now you would expect it to be gone. And what happened here is that it turns out that UTF-8 issues or redundant UTF-8 vulnerabilities were fixed in most of IIS server code base but the

components that were related to WebDav were not fixed. So, if IIS is somehow convinced to relay the request to the WebDav component then UTF-8 vulnerability comes to play and one then can bypass access controls. So, this is quite amazing, but I think it's a good lesson for us. UTF-8 vulnerability is a good lesson for us, probably talk about it in a second.

Brian Contos: Well, certainly the fact that the core code in most cases has been addressed. But of course there is core code and then there is a much bigger code base with all the additional add-ons. Is this something that you think was just simply overlooked, or they knew about this vulnerability and they just didn't bother to fix it, or you think they were seriously caught off guard because as you said UTF-8 code, these redundant vulnerabilities have been around for sometime.

Amichai Shulman: Well, we can guess together. It could have been missed; someone could have thought that the flow of the information through the servers is such that it will not be relevant. And when it gets to that point in the code...or you know someone added some support for something along the years and the code that was introduced was code that is still vulnerable to UTF-8. There are a thousand ways where programmers can make mistakes. The thing is that once you know that redundancy UTF-8 is a problem, you want to make sure in a single place in your system that redundant UTF-8 doesn't go in.

And if you go and try to do it through coding, then you are bound to find yourself in this kind of situation. Because there will always be that piece of code that you missed, or that flow of information that you overlooked, or that new code that was added by that inexperienced programmer that didn't know about redundancy UTF-8.

Brian Contos: At the more general level you explained what needs to be done. Let's assume that you've got a vulnerable code. You don't have the resources to actually go in and perhaps patch or fix the code to address this problem today. What are some of the other things that an organization can do to protect themselves?

Amichai Shulman: Well I think that by now most organizations have the choice of using the Web Application Firewall. And the Web Application Firewall is in front of the web server and actually scrutinizes each and every request coming into the server. The first thing that our Web Application Firewall is doing when scrutinizing requests is looking into encoding issue, we have introduced the protection of redundant UTF-8 encoding three years ago. Since you introduced it once and put it in front one of the applications it doesn't measure how much code you add into your application, you are protected against this type of vulnerabilities.

Brian Contos: So, in terms of the Imperva SecureSphere WAF, we've been protecting from this type of vulnerability for over three years now?

Amichai Shulman: Yeah.

Brian Contos: What are some of the lessons learned from this bad sequel to a horror movie?

Amichai Shulman: I think this example or sequel movie, I think that we should always remember that all vulnerabilities are going to come and hunt us. The fact that they are old doesn't make them inefficient, doesn't make them extinct. Coding related issues are going to resurface once and again. And we have to find more efficient solutions for these kinds of problems and we can never ignore them saying, "Well, programmers today write better codes, or programmers today will never make that mistake," -- they will.

Microsoft IIS WebDAV Remote Authentication Bypass with Amichai Shulman

So, that's the first lesson and it takes us to the place where you need alternative protection mechanisms that would allow you to mitigate this kind of vulnerability, this technical vulnerability in a single point in front of all your application codes and doesn't really bother anymore with the potential risks as a consequence of new codes or old codes that were overlooked.

Brian Contos: You know the interesting thing about this is that it almost sounds like it's just an advertisement for WAF, but it's not what we are not saying, but actually is an advertisement for WAF. [laughs] Because we're saying -- your code --

Amichai Shulman: Oh yeah. Thank you, Microsoft.

Brian Contos: [laughs] To your point earlier your code is only going to be so good and as it expands and becomes more complex and multiple people get involved, the risk of having a vulnerability becomes higher and higher. And so it will be the longer if it sits out there. And augmenting even the best code with secondary protection mechanisms, in this case a Web Application Firewall, it just makes perfect sense. It's a safety measure that's in place and like you've said, if that safety measure was in place for these organizations that have this vulnerability they wouldn't be protected right now.

Amichai Shulman: Exactly.

Brian Contos: Well, Amichai thank you so much for jumping on this podcast with me today and I know this is a very hot topic. Hopefully our listeners will be able to tune in and gain some insightful knowledge from us.

Amichai Shulman: Thank you Brian for the opportunity.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200