An Exchange zero day vulnerability

An Exchange zero day vulnerability was just announced Tuesday March 2nd. The vulnerability allows full webshell access to the server. Microsoft just issued an emergency patch Tuesday night. Below is some information, including recommendations to see if your server has been compromised.

Patch links: https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

Initial Blog post: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

We're currently finding a significant number of webshells within the "C:\inetpub\wwwroot\aspnet_client\system_web" directory. Please keep in mind, this location can be redirected via the "PathWWWRoot" value in the "HKLM\SOFTWARE\Microsoft\InetStp" registry key. Webshell file names include:

- FU7Vif5K.aspx
- ICK4sMeJ.aspx
- jFabdYwZ.aspx
- hjmQWreC.aspx
- CX47ujQS.aspx
- gwVPU69R.aspx
- M2gRp7Zo.aspx
- XJrBqeul.aspx
- Tx2tWFMb.aspx

However, we're also finding webshells in the following locations:

- C:\inetpub\wwwroot\aspnet_client\supp0rt.aspx
- C:\inetpub\wwwroot\aspnet_client\HttpProxy.aspx