

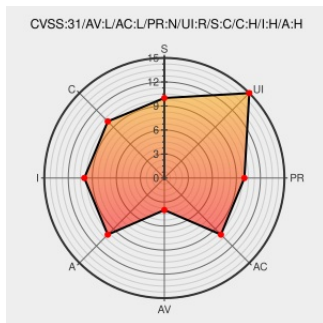


# CVE-2020-16087

Published on: 08/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:49 PM UTC

## CVE-2020-16087

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Windows](#) from [Microsoft](#) contain the following vulnerability:

An issue was discovered in Zalo.exe in VNG Zalo Desktop 19.8.1.0. An attacker can run arbitrary commands on a remote Windows machine running the Zalo client by sending the user of the device a crafted file.

CVE-2020-16087 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.6 - HIGH**

| Attack Vector  | Attack Complexity      | Privileges Required | User Interaction    |
|----------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **9.3 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                                                                                            | Tags                                                                                                                                | Link                                                                                 |
|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| ThreatSpike Blog: Remote Code Execution in a Popular Chat App: Easy as Sending a File (CVE-2020-16087) | <a href="#">Exploit</a><br><a href="#">Third Party Advisory</a><br><a href="#">www.threatspike.com</a><br><a href="#">text/html</a> | <a href="#">MISC</a><br><a href="#">www.threatspike.com/blog/cve-2020-16087.html</a> |

There are currently no QIDs associated with this CVE

| Type                                             | Vendor    | Product      | Version  | Update | Edition | Language |
|--------------------------------------------------|-----------|--------------|----------|--------|---------|----------|
| Operating System                                 | Microsoft | Windows      | -        | All    | All     | All      |
| Operating System                                 | Microsoft | Windows      | -        | All    | All     | All      |
| Application                                      | Vng       | Zalo Desktop | 19.8.1.0 | All    | All     | All      |
| Application                                      | Vng       | Zalo Desktop | 19.8.1.0 | All    | All     | All      |
| cpe:2.3:o:microsoft:windows:-:*.***.***.*:       |           |              |          |        |         |          |
| cpe:2.3:o:microsoft:windows:-:*.***.***.*:       |           |              |          |        |         |          |
| cpe:2.3:a:vng:zalo_desktop:19.8.1.0:*.***.***.*: |           |              |          |        |         |          |
| cpe:2.3:a:vng:zalo_desktop:19.8.1.0:*.***.***.*: |           |              |          |        |         |          |

No vendor comments have been submitted for this CVE