**CYBER DEFENSE AFRICA**: SECURITY ANNOUNCEMENT **Date**: 31/05/2022

| Content Type | Description |
|---|---|
| Title | *Zero-day in Microsoft's Office suite* |
| Id | *202205/Alert/04* |
| Code LTP | *White* |
| Risk Level | *High* |
| Affected Application and Service | *Microsoft Office* |
| Version | *2013, 2016, 2019, 2021 and Professional Plus versions* |
| Platform | *Na* |
| Update | *Na* |
| Summary | *Vulnerability That Could Allow Arbitrary Code* Execution *with Calling Application Privileges on Affected Systems* |
| Impacts | *An attacker who successfully exploited this vulnerability could:*<br>- *Install programs*<br>- *View, edit, or delete data*<br>- *Creates new accounts in the context allowed by the user's rights.* |
| Detailed Description | *The Zero-day vulnerability, which is now assigned the identifier CVE-2022-30190, is rated 7.8 out of 10 for severity in the CVSS vulnerability scoring system.*<br>*The vulnerability occurs when the Microsoft Support Diagnostic Tool (MDST) is called using the URL protocol from a calling application such as Word.* |
| Solutions | *In order to protectcustomers, Microsoft has published on their website tips to apply (click on the second link in* ***links for more details****)* |
| **Links for more details** | *https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190*<br>*https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/* |