

## ATTENTION IT STAFF

Due to last week's security breach we need to rebuild some of our core servers. This has impacted a handful of our workstations, update services, monitoring tools and backups. As we work to rebuild, please assist our NOC by e-mailing a link to any internal web applications to [itsupport@outdated.htb](mailto:itsupport@outdated.htb) so we can get them added back into our monitoring platform for alerts and notifications.

We have also onboarded a new employee to our SOC to assist with this matter and expedite the recovery of our update services to ensure all critical vulnerabilities are patched and servers are up to date. The CVE list below is top priority, and we must ensure that these are patched ASAP.

Thank you in advance for your assistance. If you have any questions, please reach out to the mailing list above.

CVE ID	Type	Publish Date	Score	Access	Complexity	Description
<a href="#">CVE-2022-30190</a>	Exec Code	2022-06-01	9.3	Remote	Medium	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability.
<a href="#">CVE-2022-30138</a>	Exec Code	2022-05-18	7.2	Local	Low	Windows Print Spooler Elevation of Privilege Vulnerability.
<a href="#">CVE-2022-30129</a>	Exec Code	2022-05-10	6.8	Remote	Medium	Visual Studio Code Remote Code Execution Vulnerability.
<a href="#">CVE-2022-29130</a>	Exec Code	2022-05-10	9.3	Remote	Medium	Windows LDAP Remote Code Execution Vulnerability.
<a href="#">CVE-2022-29110</a>	Exec Code	2022-05-10	9.3	Remote	Medium	Microsoft Excel Remote Code Execution Vulnerability