BlueOrange Alert:

On-Premise Exchange Critical Vulnerability

In March of 2020, the Department of Homeland Security's Cybersecurity Infrastructure and Security Agency published an alert about CVE-2020-0688, an On-Premise Exchange Server vulnerability which allows attackers with remote credentials to execute remote commands on unpatched servers.

The vulnerability relies on non-unique security keys which are created by the server during the installation phase. An attacker with stolen credentials could then pass through the Exchange Web Service, which runs in system context.

The main risks of this vulnerability include the following:

- Stolen accounts used for this exploit do not need to be Exchange administrator accounts or otherwise highly privileged.
- This vulnerability provides full access to the server running Exchange as though the attacker had administrative credentials
- Compromised servers can be used to stage further attacks against the rest of the environment.

It is critical to update Exchange environments to currently supported versions and to patch following Microsoft's recommendations in order to secure against this exploit. Microsoft's recommendations can be found here: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0688

Further reading on the subject is available at the following links:
https://www.us-cert.gov/ncas/current-activity/2020/03/10/unpatched-microsoft-exchange-servers-vulnerable-cve-2020-0688
https://blog.rapid7.com/2020/04/06/phishing-for-system-on-microsoft-exchange-cve-2020-0688/

About BlueOrange Compliance:

BlueOrange Compliance specializes in assisting healthcare organizations navigate HIPAA and HITECH privacy and security requirements. Complex, ever-changing healthcare regulations and increasing risks make it difficult for organizations to stay in front of emerging cyber threats. As a single source, we equip every client with affordable, practical, comprehensive privacy and security solutions, including multiple sources of information to help manage risk. Our clients have peace of mind knowing they are compliant and prepared for potential breaches and adverse audits. BlueOrange Compliance provides this alert for educational purposes only without warranty and specialized advice should be sought about your specific circumstances.