AREA 1

AREA 1 SECURITY ADVISORY

EXIM VULNERABILITY

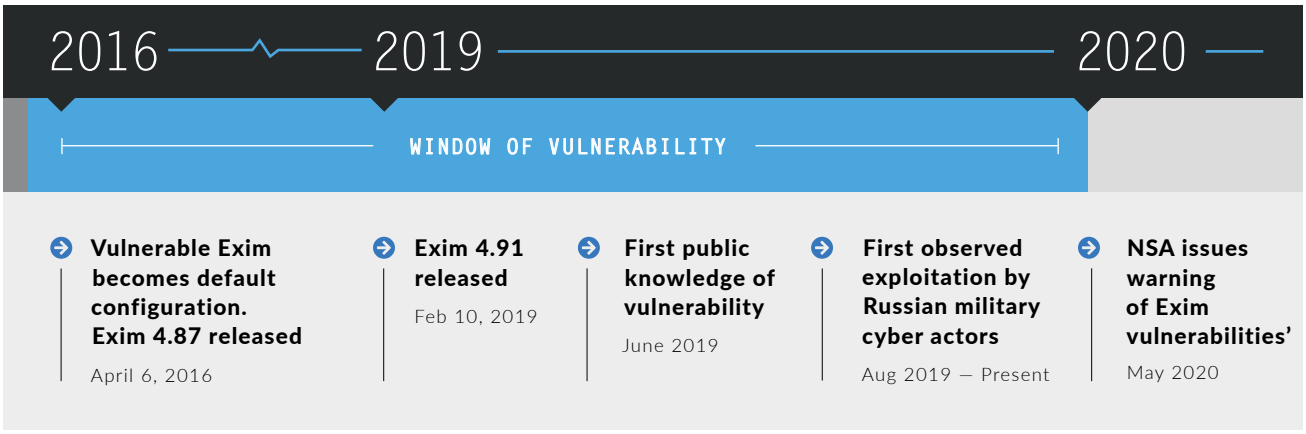
Advisory Details

On Thursday, 28 May 2020 the National Security Agency issued a Cybersecurity Advisory warning that cyber actors linked to the Russian military have been exploiting a critical vulnerability CVE-2019-10149 in Exim mail transfer agent (MTA) software since at least August of 2019.

Millions of Exim servers appear on the internet, and more than 300,000 Exim servers (62.57% of which are hosted in the United States) are currently exposed to the CVE-2019-10149 critical vulnerability. CVE-2019-10149 impacts versions of Exim 4.87 thru 4.91.

The exploitation of which allows the adding of privileged users, disabling network security settings, launching BEC phishing campaigns, as well as broader network exploitation.

The specific remote code execution vulnerability in CVE-2019-10149 became the default configuration in Exim version 4.87 on 6 April 2016, leaving a wide window of potential compromise between then and when the vulnerability was disclosed and available for mitigation in Exim versions 4.92 and later on 10 February 2019.



Area 1 Security has observed vulnerable Exim servers being run at foreign ministries, leading public policy think tanks, major research institutions, and in the Amazon Gov Cloud. Within the United States Government Exim servers that are vulnerable to CVE-2019-10149 exploitation have been identified within the State Department networks, various state and local government networks, such as Lewisburg, Tennessee, the Township of Ocean in New Jersey, and Paducah, Kentucky.

An extensive list of Exim servers vulnerable to CVE-2019-10149 as of 1 June 2020 is provided here.

This Russian cyber actor is the same that interfered in prior United States elections. Area 1 Security has identified at least 44 candidates for public office in the 2018 United States Elections that were running vulnerable Exim servers, and at least 50 candidates for public office in the 2020 United States Elections currently running Exim servers. Incumbent candidates' in the 2020 elections were assuredly susceptible to CVE-2019-10149 during the 2018 elections, and prior to February 2019.

FIRST NAME	LAST NAME	OFFICE	PARTY
Jim	Banks	U.S. House Indiana District 3	Republican Party
Tom	Suozzi	U.S. House New York District 3	Democratic Party
Jaime	Beutler	U.S. House Washington District 3	Republican Party
Mo	Brooks	U.S. House Alabama District 5	Republican Party
Jim	Hagedorn	U.S. House Minnesota District 1	Republican Party
Paul	Tonko	U.S. House New York District 20	Democratic Party
H. Morgan	Griffith	U.S. House Virginia District 9	Republican Party

Example of Incumbent U.S. Candidates running Exim as of 1 June 2020

AREA 1

SECURITY RECOMMENDATIONS

Area 1 Security Recommendations

1. **Given the government's guidance to update Exim immediately by installing version 4.93 or newer to mitigate CVE-2019-10149 and other vulnerabilities including but not limited to CVE-2019-15846 and CVE-2019-16928, we're urging candidates to cease use of Exim in their campaigns. The persistent nature of these exploitations means that upgrading alone does not mitigate exploitation; this, coupled with the outsourced management of IT infrastructure and prior Russian cyber activities directed towards U.S. elections, make use of Exim by campaigns ill advised.**

2. Network administrators across non-election sensitive organizations should also note that upgrading Exim does not remediate prior exploitation. Additionally, if a specific Exim server on a network isn't designated for primary or critical usage; it's likely that it may have missed ongoing upgrade/update cycles and may have been unpatched through this period. That represents a specific advantage to cyber actors who leverage any vulnerability to gain a foothold within the organization and then move laterally within the network to achieve their objectives.

3. Running your own custom email infrastructure requires network administrators to be perfect every single day. We recommend use of cloud email infrastructure such as Google's GSuite or Microsoft's Office 365 in combination with a cloud email security solution.

4. If you continue running Exim, update to the latest version, running a version prior to 4.93 leaves a system vulnerable to disclosed vulnerabilities. Administrators can update Exim Mail Transfer Agent software through their Linux distribution's package manager or by downloading the latest version from https://exim.org/mirrors.html.

5. Network administrators who find Exim servers on their networks, not for official use, should work to eliminate them from the network.

About Area 1 Security

Area 1 Security is the first to bring accountability to cybersecurity. Backed by top-tier investors, Area 1 Security is led by security, Artificial Intelligence, and data analytics experts who created a preemptive solution to stop phishing, the number one cause of cyber attacks.

Area 1 Security works with organizations worldwide, including Fortune 500 banks, insurance, and tech companies, and healthcare providers to realign their cybersecurity posture for combating the most significant risks, protecting customer data, and stopping attacks before they happen. Area 1 Security is a recipient of Inc. Magazine's "2018 Inc.'s Best Workplaces" in America. To learn more about Area 1 Security, visit **www.area1security.com**, join the conversation at **@area1security** or follow the **blog** for the latest industry news and insights on how to stop phishing.

▸ **Learn More** INFO@AREA1SECURITY.COM