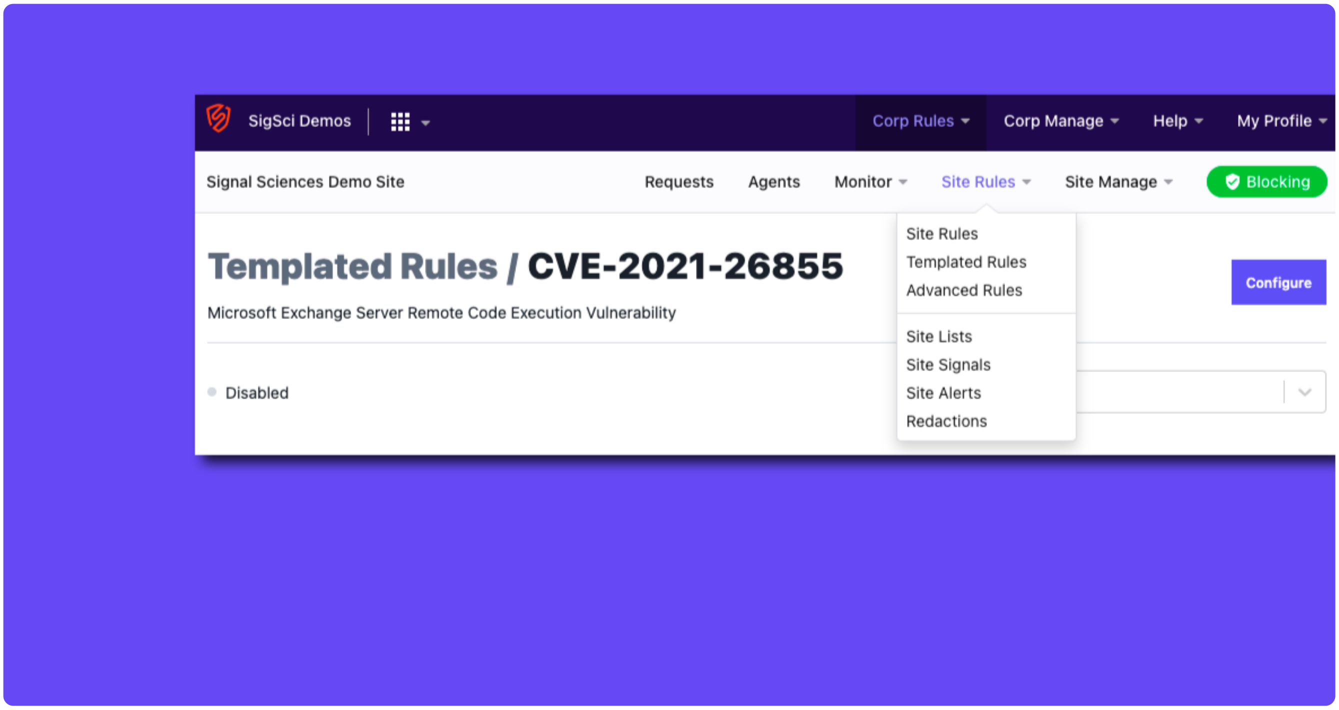


Templated Rules / CVE-2021-26855

Microsoft Exchange Server Remote Code Execution Vulnerability

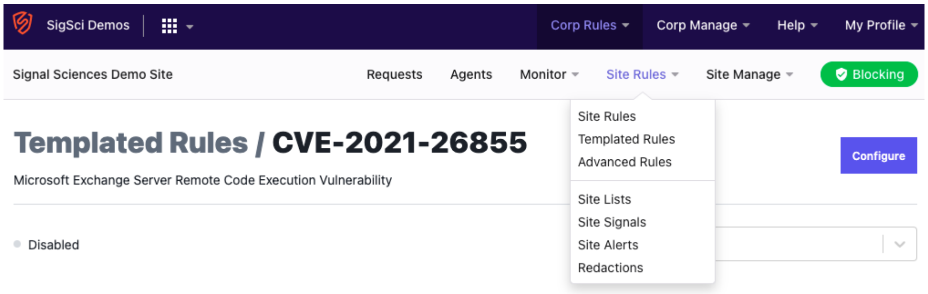
Disabled

INFORMATION SECURITY, WEB APPLICATION SECURITY

Next-Gen WAF protection for recent Microsoft Exchange vulnerabilities

Protecting our customers

Our security research team has built and deployed a rule to protect Fastly's Signal Sciences Next-Gen WAF customers against the recently announced Microsoft Exchange Server vulnerabilities. The custom rule is available in the console under "Templated Rules".



Templated Rules / CVE-2021-26855

Microsoft Exchange Server Remote Code Execution Vulnerability

Disabled

We strongly suggest that customers using Signal Sciences Next-Gen WAF in front of their Microsoft Exchange servers enable this rule as soon as possible and configure it to block requests if the signal is observed. Additionally, follow all guidance from Microsoft to patch affected systems. The vulnerabilities in question are actively being exploited globally and have severe impact.

Patching Microsoft Exchange systems

We are seeing a large uptick in exploitation attempts in the wild. This is an evolving story and our teams are working continuously to ensure the rules are catching the latest attacks, but this should not be your only line of defense. We strongly recommend that you patch affected systems, perform incident response, and follow recommendations from Microsoft.

Exploit chain

The observed attacks on Microsoft Exchange systems chain together multiple CVEs (Common Vulnerabilities and Exposures) to carry out the attack. The impact of these attacks range from full system takeover through Remote Code Execution (RCE), as well as email inbox exfiltration and compromise. At a high level, the exploit chain is carried out as follows:

1. A Server-Side Request Forgery (SSRF) vulnerability in Microsoft Exchange Server identified as CVE-2021-26855 allows attackers to send HTTP requests to the exposed Exchange server and access other endpoints as the Exchange server itself. This is an unauthenticated step of the attack which makes the vulnerability exceptionally easy to exploit.
2. An insecure deserialization vulnerability identified by CVE-2021-26857 leverages the SYSTEM-level authentication obtained by the above SSRF attack to send specially-crafted SOAP payloads which are insecurely deserialized by the Unified Messaging Service. This gives the attacker the ability to run code as SYSTEM on the Exchange server.

3. After CVE-2021-26855 is successfully exploited, attackers can then utilize CVE-2021-27065 and CVE-2021-26858 to write arbitrary files to the Exchange server itself on any path. This code that is uploaded by the attacker is run as SYSTEM on the server. Lateral movement, malware implanting, data loss, escalation, and more can be carried out through these vulnerabilities.

By enabling the Signal Sciences Next-Gen WAF templated rule, the first step in the exploit chain cannot be carried out. If you would like to dig deeper into the technical details of this chain of attacks please see this post by the folks at Praetorian. To enable the templated rule, please refer to our documentation for details on how to enable templated rules.