

Finding GTN-008: Stored Cross Site Scripting (XSS) at 'Blacklist' endpoint

Severity: High Vendor of the product: MDaemon Technologies Product: SecurityGateway for Email Servers Version: v8.5.2 (64 bit) Researcher: Pankaj Kumar Thakur (Green Tick Nepal Pvt. Ltd.)

Details of Vulnerability:

The payload '"<script>alert(1)</script>' was submitted with POST Request. The HTTP response appears to contain the output from the injected payload, indicating that the payload was executed successfully on the server.

Impact:

XSS attacks can expose the user's session cookie, allowing the attacker to hijack the user's session and gain access to the user's account, which could lead to impersonation of users.

Evidence:

DecurityGateway						pankaj@pankaj 🕜 Help 🚯 About 🕩 Si
	Anti-Spam	>	Addresses Blacklist			
MAIN	Anti-Virus	>	😔 New 🕼 Edit 😵 Delete 🛛 Q. Search 📤 Import 📤 Export			For Domain: Glob
	Anti-Spoofing	>	Select an item from the list below and then select an option from the toolbar above to manage that list item.			
SETUP / USERS	Anti-Abuse	>	Value		Comment	
	RMail™		✓ test@test.com	"> <script>alert(1)</script>		
	Data Leak Prevention	>				
	Filtering	>				
MESSAGES	Blacklists	~				
/ QUEUES	Addresses					
I	Hosts					



Inject XSS payload at comment parameter while Address Blacklisting

Now visit

http://localhost:4000/SecurityGateway.dll?view=block_and_white_lists&list=1&blacklist=1&user=ProbePhishing&load Data=1



Suggested Remediation:

- Sanitize all the user supplied inputs before executing them. Your application code should never blindly output the result of input data received without validation.
- URL encoding must be done before inserting untrusted data into HTML URL parameter values.
- JavaScript encoding must be done before inserting untrusted data into JavaScript data values.
- Encode CSS scripts and strict validation before inserting untrusted data into HTML style property values must be done.