From: Telstra Security Operations
To: nbn Team (nbn@email.com)
Subject: Create Firewall Rule to Block /tomcatwar.jsp
—
Body:
Hello nbn Team,

We would like to request the creation of a firewall rule and provide you more information about the ongoing attack.

Between 3:16:34 AM to 3:21:00 AM UTC on March 20, 2022, there was an automated coordinated attack on “/tomcatwar.jsp”

I would like to request to block traffic attempts on the endpoint “/tomcatwar.jsp” for the meantime while resolving the issue.

The attacker appears to be utilizing a Python script to exploit a vulnerability in our system. This script sends crafted HTTP POST requests to specific endpoints, including "tomcatwar.jsp," with malicious payload data embedded in the request body.

Upon successful exploitation, the attacker may gain unauthorized access to our system, potentially leading to data breaches, system compromise, or disruption of services.
We're taking immediate action to mitigate this threat, including implementing firewall rules to block access to vulnerable endpoints and conducting a thorough review of our web application security measures.

For any questions or issues, don’t hesitate to reach out to us.

Kind regards,
Telstra Security Operations