### **Summary**

On 20 Mar, 2002 at approximately14:00, a malware attack targeting Spring Framework applications was detected. The attack exploited the Spring4Shell vulnerability, allowing attackers to execute arbitrary code on vulnerable systems. This resulted in unauthorized access to critical infrastructure and potential data compromise.

The attack primarily focused on [specific URLs or paths] within the Spring applications, using [HTTP methods] and sending a [specific payload]. Firewall logs indicated a significant spike in "Bypass" events, suggesting successful attempts to bypass security controls.

### **Impact**

The malware attack had a significant impact on [list of affected systems or services]. This disruption caused [specific consequences, e.g., service outages, data loss, financial losses].

The compromised systems may have been used as a foothold to further compromise other systems within the network, increasing the potential damage. Additionally, the exposure of sensitive data could have severe consequences, such as identity theft, financial fraud, or reputational harm.