ACME Anvils
Log File Report

SOC Team

October 26, 2023

It has been brought to our attention that there has been a breach in the company's network. Recent log files have been collected and reviewed for any information that may be relevant to the recent breach. The goals of the task at hand are:

- To collect recent log files regarding the breach
- Review recent log files for any suspicious activity
- Report our findings to assist in resolving the breach

ACME IDS

Within the Intrusion Detection System log files there were numerous logs that may be relevant to the recent breach in the company's network. To begin, there were eighty counts of detected spyware activity, both outbound and external, originating from multiple hosts within the company network. Spyware is a type of malware designed to gain access to or damage your computer without your knowledge. It can steal your sensitive information and relay it to advertisers, data firms or external users. There were also four counts of "Invalid Transport Field". This message appears when there is an invalid transport number, which usually just means there is an invalid port number. But, if these messages proceed, it can be related to a Denial of Service attack. Most importantly, there were 1,272 counts of a Potential Vulnerability Exploit Allowed, both outbound and external. A number of hosts were impacted from these events. Applications such as HTTPS, DNS, SIP, IMAPS, SMTP, POP3, SSH, Microsoft Directory Services, End Point Mapper, and FTP were also impacted due to these events.

ACME Brocade

The findings of the ACME Brocade Log Files were concerning. All of the information found within the logs were readable besides the actual log messages, which are the most important aspect. Without them, we can only know the timestamps, hosts, classifications and zones. The contents of log files should always be readable, especially on your own system. This leaves us questioning the core details of the security event itself. These are major red flags. For the SOC Team to be able to respond to a security event , and mitigate if needed, the details of such an event must be available. It is possible an attacker may have executed log tampering, log poisoning , or even a log injection attack. These attacks could result in an attacker running arbitrary code on the server, forge log entries, corrupt the log format, or even just simply making it difficult to detect or investigate an attack.

Conclusion

In this report, there is a detailed description of the recent log files that were collected for ACME Anvils. The SOC Team here at ACME Anvils collected all log files that may be relevant to the recent breach in the company's network. These log files were thoroughly reviewed and assessed for suspicious activity within the company's network. Any activity deemed to be suspicious by the SOC Team was reported.