JASK

THREAT ADVISORY

CVE-2018-1050/1057 SAMBA Protocol vulnerabilities

AUTHOR
ROD SOTO

JASKLABS
TA-0008

TLP
WHITE

RISK FACTOR
HIGH

THREAT ADVISORY

CVE-2018-1050/1057
SAMBA Protocol vulnerabilities

AUTHOR
ROD SOTO

JASKLABS
TA-0008

TLP
WHITE

RISK FACTOR
HIGH

Overview

A new set of vulnerabilities affecting SAMBA, a network protocol for file sharing and printing services, has been disclosed. SAMBA is an open-source software and is included in every *nix distribution available, making it a standard service for the majority of *nix installations in organizations. These services are needed for basic file sharing and printing services and become, in many cases, "hubs" of multiple documents and printing traffic, which makes them valuable targets for malicious actors. The new vulnerabilities disclosed allow Denial of Service (CVE-2018-1050) where service will shutdown or cease to function and CVE-2018-1057, which allows an unprivileged user to change passwords.

SAMBA is also embedded in many devices, from NAS systems, printers, DVRs, entertainment home file sharing and more. It is known that these devices usually store lots of files and, in many cases, become the main file sharing and printing resource of many organizations. These two new vulnerabilities are likely to be used as post-exploitation payloads, as SAMBA is mainly a service used inside the perimeter. However, the ability to either deny service or change credentials can facilitate lateral movement and exfiltration of data too.

Indicators

Attacking file sharing and printing services is not uncommon as recently seen in exploits such as EternalBlue and EternalRed/SambaCry, which caused a good amount of compromises and were coupled with Ransomware in many campaigns. This combination of a data hub and the ability to possibly change credentials, and then execute on it, makes these two new vulnerabilities possible candidates to replicate past attack vectors.

Compromised SMB shares can be used for many malicious activities such as to steal sensitive information stored or in transit in specific devices and to pivot and move laterally from unsuspecting devices as well (NAS, Printers). In addition, many devices are placed on networks with default, or weak, credentials which may allow attackers with these type of exploits to run code and proceed to execute malicious activities, such as cryptomining or installing ransomware and proceeding to demand ransom payments.

AUTHOR
ROD SOTO

JASKLABS
TA-0008

TLP
WHITE

RISK FACTOR

HIGH

Affected versions for these vulnerabilities are:

CVE-2018-1050

All versions of Samba from 4.0.0 onwards.
Not Vulnerable: Samba 4.7.6, 4.6.14, 4.5.16
Summary: Missing null pointer checks may crash the external print server process.

CVE-2018-1057

All versions of Samba from 4.0.0 onwards.
Not Vulnerable: Samba 4.7.6, 4.6.14, 4.5.16
Summary: On a Samba 4 AD DC any authenticated user can change other users' passwords over LDAP, including the passwords of administrative users and service accounts.
(Note: This vulnerability impacts SAMBA as file services role and also as part of an MS Active directory environment). More detailed information on Packet Storm.

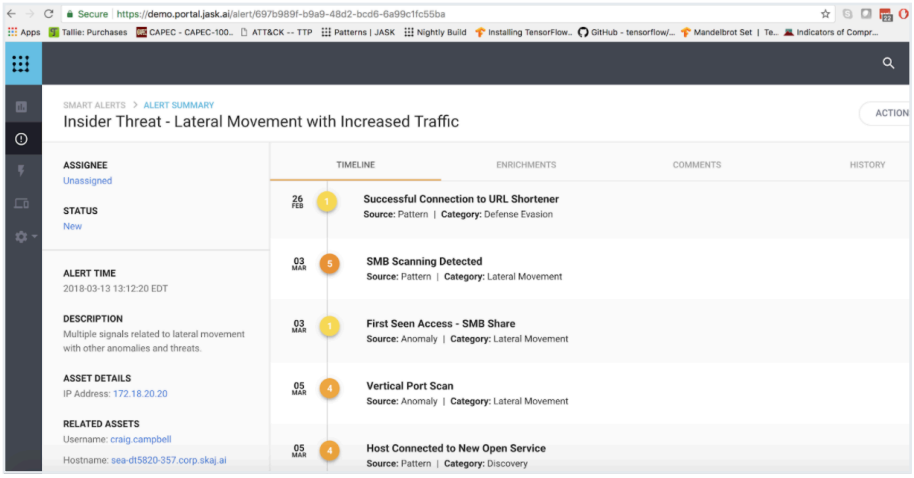
Lab/Field Study

Due to embargo, we will not be publishing content in this section until a later date. Please check back for updates.

JASK Detection

JASK's ASOC platform possesses several mechanisms to detect these threats. As outlined above, these vulnerabilities will be used as post-exploitation payloads. As such, they can be detected as part of the exploitation chain. This exploitation chain detection by JASK ASOC allows analysts to place together a visual representation of the elements related to possible exploitation of SMB/SAMBA services.

Figure Shows JASK ASOC Smart Alert



The above figure shows a JASK ASOC Smart Alert where SMB/SAMBA port/service scanning is detected after a user has connected to a suspicious URL shortener, then accessing a file share that this user had not previously accessed before.

AUTHOR
ROD SOTO

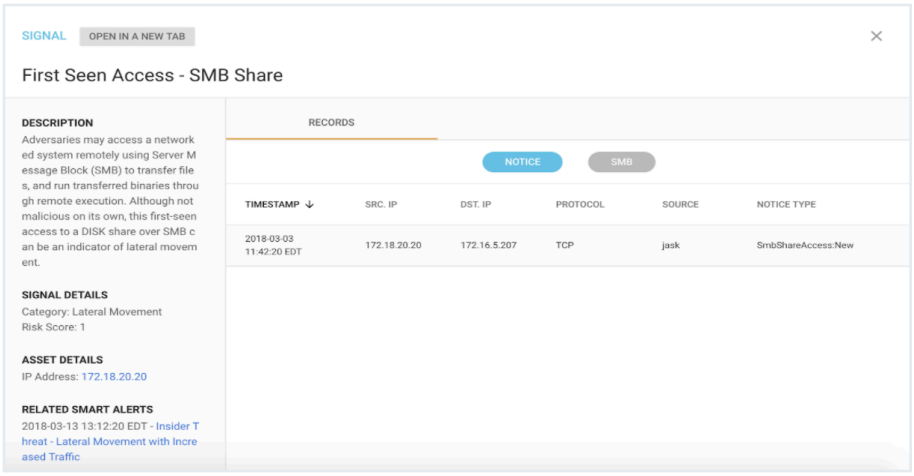
JASKLABS
TA-0008

TLP
WHITE

RISK FACTOR
HIGH

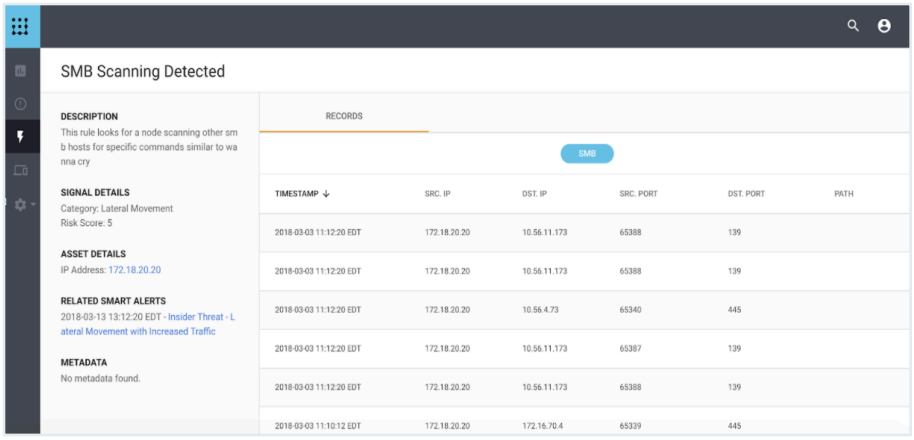
This may indicate, depending on this particular user's patterns and privileges, that a post-exploitation payload may have been used to grant access from the user's account/device to a targeted device running SMB/SAMBA services. The following figure shows such individual signal.

Figure Shows First Seen Access signal



JASK ASOC can also detect port/service scans of SMB/SAMBA services and display a specific and detailed visual interface that provides analysts with situational awareness. The figure below shows origin and targeted ports/services and hosts.

Figure Shows First Seen Access signal



By providing these simplified situational awareness items, analysts can spot suspicious activity, and even exploitation, without having the attack signatures (which can be difficult to obtain), as they are vendor-dependent and many times subjected to publication embargoes.

AUTHOR
ROD SOTO

JASKLABS
TA-0008

TLP
WHITE

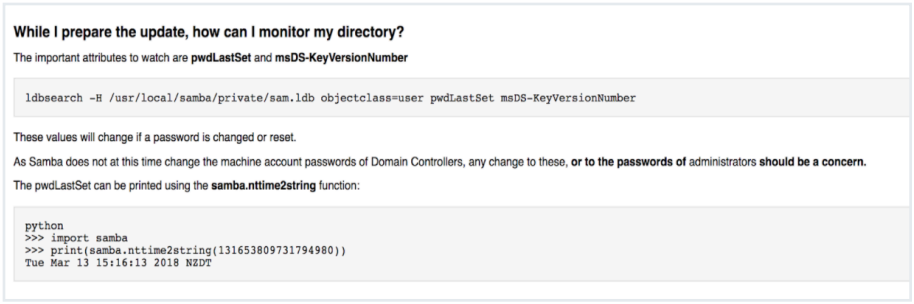
RISK FACTOR
HIGH

Mitigation

According to vulnerability reports and advisories, it is recommended to update any devices running SAMBA as soon as possible. SAMBA's security page provides details of all patches available to date and the corresponding CVEs.

Per SAMBA's security page, the following graphic displays currently available ways to monitor for these type of vulnerabilities/exploitations. Specifically, the password reset one is the most useful for lateral movement and escalation of privileges as of the writing of this advisory.

Figure shows suggested monitoring commands



It is also important to note that no useable logs in the SAMBA implementation currently exist that allow detection of suspicious/malicious password reset activity, and resetting accounts with high privileges may not prevent further escalation from this attack. Because of this, contextual monitoring can provide ways of detecting it.

Possible workarounds

The SAMBA security page offers a number of workarounds to mitigate the exploitation of CVE-2018-1057. However, many of these workarounds can result in changes that may affect related services significantly in organizations and should be taken as a guide to be adapted with very specific configurations to local environment.

It is important for organizations to weigh disabling/deprecating services that may affect overall operations with the level of risk of exploitation from these vulnerabilities.

About JASK

JASK is modernizing security operations to reduce organizational risk and improve human efficiency. Through technology consolidation, enhanced AI and machine learning, the JASK Autonomous Security Operations Center (ASOC) platform automates the correlation and analysis of threat alerts, helping SOC analysts focus on high-priority threats, streamline investigations and deliver faster response times.

www.jask.ai