Template - Suspicious network connection over Encrypting File System Remote Protocol

Link to alert

**Description**

Adversaries may exploit the Encrypting File System Remote Protocol to improperly perform privileged file operations. In this attack, the attacker can escalate privileges in an Active Directory network by coercing authentication from machine accounts and relaying to the certificate service. This attack allows an attacker to take over an Active Directory (AD) Domain by exploiting a flaw in the Encrypting File System Remote (EFSRPC) Protocol and chaining it with a flaw in Active Directory Certificate Services.

**Classification**: Incident

**How to investigate**

<https://docs.microsoft.com/en-us/defender-for-identity/lateral-movement-alerts#suspicious-network-connection-over-encrypting-file-system-remote-protocol-external-id-2415>

**Alert detail**

Date:

Source Computer (used by actor):

File host:

File path:

Domain controllers (used to authenticate):

Severity: High

**Remediation**

Check if the source computer is running an attack tool such as ADCSPwn, or if the originating device is a network scanner.

Investigate the file name the attacker was trying forcing the authentication with.

Investigate the target domain controller and identify activities that occurred after the attack.

If the breach is confirmed:

* Contain the Device for the remediation
* Search for the tool that potentially performed that the attack and remove it.

**Mitigation**

* Disable or Remove Feature or Program - Minimize available services to only those that are necessary.
* Exploit Protection - Security applications that look for behaviour used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behaviour
* Privileged Account Management - Minimize permissions and access for service accounts to limit impact of exploitation
* Update Software - Update software regularly by employing patch management for internal enterprise endpoints and servers.
* Vulnerability Scanning - Regularly scan the internal network for available services to identify new and potentially vulnerable services.

***NB: PROVIDE A SCREESNHOT OF THE WORK DONE***