什么“某人尝试劫持加密连接”错误含义？

目录

简介

本文描述错误“很可能，某人尝试劫持对远程主机的加密连接”，并且承担的更正的步骤您的思科给安全工具(ESA)和Cisco安全管理设备(SMA)发电子邮件。

什么“某人尝试劫持加密连接”错误含义？

当您配置您的与您的SMA时的ESA通信，您也许发现此错误：

```
Error - The host key for 172.16.6.165 appears to have changed.
It is possible that someone is trying to hijack the encrypted
connection to the remote host.
Please use the logconfig->hostkeyconfig command to verify
(and possibly update) the SSH host key for 172.16.6.165.
```

当ESA替换并且使用主机名和IP地址和原始ESA一样时，这能发生。用于通信和验证的以前存储的SSH密钥在ESA和SMA之间在SMA存储。SMA然后看到ESA通信路径更改，并且相信未授权的源当前是由IP地址控制assocaited对ESA。

为了更正此，请登陆对SMA的CLI，并且完成这些步骤：

1. 输入**logconfig**命令。
2. 输入**hostkeyconfig**。
3. 输入**删除**并且选择在ESA IP的当前安装的主机密钥列表关联的编号。
4. 返回到主CLI提示符并且输入**commit命令**。

```
mysma.local> logconfig

Currently configured logs:
Log Name Log Type Retrieval Interval
-----------------------------------------------------------------------------
1. authentication Authentication Logs FTP Poll None
2. backup_logs Backup Logs FTP Poll None
3. cli_logs CLI Audit Logs FTP Poll None
4. euq_logs Spam Quarantine Logs FTP Poll None
5. euqgui_logs Spam Quarantine GUI Logs FTP Poll None
6. ftpd_logs FTP Server Logs FTP Poll None
7. gui_logs HTTP Logs FTP Poll None
8. haystackd_logs Haystack Logs FTP Poll None
9. ldap_logs LDAP Debug Logs FTP Poll None
10. mail_logs Cisco Text Mail Logs FTP Poll None
```

```
11. reportd_logs Reporting Logs FTP Poll None
12. reportqueryd_logs Reporting Query Logs FTP Poll None
13. slbld_logs Safe/Block Lists Logs FTP Poll None
14. smad_logs SMA Logs FTP Poll None
15. snmp_logs SNMP Logs FTP Poll None
16. sntpd_logs NTP logs FTP Poll None
17. system_logs System Logs FTP Poll None
18. trackerd_logs Tracking Logs FTP Poll None
19. updater_logs Updater Logs FTP Poll None
20. upgrade_logs Upgrade Logs FTP Poll None

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> hostkeyconfig

Currently installed host keys:
1. 172.16.6.165 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA0ilM...DVc7plDQ==
2. 172.16.6.150 ssh-dss AAAAB3NzaC1kc3MAAACBAODKHq6uakiM...cooFXzLHFP
3. 172.16.6.131 ssh-dss AAAAB3NzaC1kc3MAAACBAI4LkblFtidp...WhM5XLNA==


Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> delete

Enter the number of the key you wish to delete.
[]> 1

Currently installed host keys:
1. 172.16.6.150 ssh-dss AAAAB3NzaC1kc3MAAACBAODKHq6uakiM...cooFXzLHFP
2. 172.16.6.131 ssh-dss AAAAB3NzaC1kc3MAAACBAI4LkblFtidp...WhM5XLNA==

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>

Currently configured logs:
Log Name Log Type Retrieval Interval
-------------------------------------------------------------------------------
1. authentication Authentication Logs FTP Poll None
2. backup_logs Backup Logs FTP Poll None
3. cli_logs CLI Audit Logs FTP Poll None
4. euq_logs Spam Quarantine Logs FTP Poll None
5. euqgui_logs Spam Quarantine GUI Logs FTP Poll None
6. ftpd_logs FTP Server Logs FTP Poll None
7. gui_logs HTTP Logs FTP Poll None
8. haystackd_logs Haystack Logs FTP Poll None
```

```
9. ldap_logs LDAP Debug Logs FTP Poll None
10. mail_logs Cisco Text Mail Logs FTP Poll None
11. reportd_logs Reporting Logs FTP Poll None
12. reportqueryd_logs Reporting Query Logs FTP Poll None
13. slbld_logs Safe/Block Lists Logs FTP Poll None
14. smad_logs SMA Logs FTP Poll None
15. snmp_logs SNMP Logs FTP Poll None
16. sntpd_logs NTP logs FTP Poll None
17. system_logs System Logs FTP Poll None
18. trackerd_logs Tracking Logs FTP Poll None
19. updater_logs Updater Logs FTP Poll None
20. upgrade_logs Upgrade Logs FTP Poll None

mysma.local> commit

Please enter some comments describing your changes:
[]> ssh key update
```

最后，从SMA GUI，请选择**集中化Serivces > Security伊莱克斯**然后选择在提交了原始错误的列表的ESA。 一旦选择**建立连接…**和**测试连接**，验证，创建一个新的SSH主机密钥对，并且存储在SMA的此主机密钥对。

再访SMA的CLI，并且重新运行**logconfig > hostkeyconfig**为了查看新的主机密钥对。

相关信息

- [思科电子邮件安全工具-最终用户指南]
- [Cisco安全管理设备-最终用户指南]
- [技术支持和文档 - Cisco Systems]