

Scan Report

Vulnerabilities and Exploits search started on port <PyQt5.QtCore.QModelIndex object at 0x7f4fa1

Vulnerability id: CVE-2001-0361

Type: cve

Title: cve

Score: 4.0

Description: Implementations of SSH version 1.5, including (1) OpenSSH up to version 2.3.0, (2) AppGate, and (3) ssh-1 up to version 1.2.31, in certain configurations, allow a remote attacker to decrypt and/or alter traffic via a "Bleichenbacher attack" on PKCS#1 version 1.5.

Vulnerability id: CVE-2001-0471

Type: cve

Title: cve

Score: 7.5

Description: SSH daemon version 1 (aka SSHD-1 or SSH-1) 1.2.30 and earlier does not log repeated login attempts, which could allow remote attackers to compromise accounts without detection via a brute force attack.

Exploit cvss id: MSF:EXPLOIT/UNIX/SSH/ARISTA_TACPLUS_SHELL/

Title: Arista restricted shell escape (with privesc)

Type: metasploit

Description: This exploit module takes advantage of a poorly configured TACACS+ config, Arista's bash shell and TACACS+ read-only account to privilege escalate. A CVSS v3 base score of 9.8 has been assigned.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/VYOS_RESTRICTED_SHELL_PRIVESC/

Title: VyOS restricted-shell Escape and Privilege Escalation

Type: metasploit

Description: This module exploits command injection vulnerabilities and an insecure default sudo configuration on VyOS versions 1.0.0 <= 1.1.8 to execute arbitrary system commands as root. VyOS features a `restricted-shell` system shell intended for use by low privilege users with operator privileges. This module exploits a vulnerability in the `telnet` command to break out of the restricted shell, then uses sudo to exploit a command injection vulnerability in `/opt/vyatta/bin/sudo-users/vyatta-show-lldp.pl` to execute commands with root privileges. This module has been tested successfully on VyOS 1.1.8 amd64 and VyOS 1.0.0 i386.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/APPLE_IOS/SSH/CYDIA_DEFAULT_SSH/

Title: Apple iOS Default SSH Password Vulnerability

Type: metasploit

Description: This module exploits the default credentials of Apple iOS when it has been jailbroken and the passwords for the 'root' and 'mobile' users have not been changed.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/QUANTUM_VMPRO_BACKDOOR/

Title: Quantum vmPRO Backdoor Command

Type: metasploit

Description: This module abuses a backdoor command in Quantum vmPRO. Any user, even one without admin privileges, can get access to the restricted SSH shell. By using the hidden backdoor "shell-escape" command it's possible to drop to a real root bash shell. This module has been tested successfully on Quantum vmPRO 3.1.2.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/QUANTUM_DXi_KNOWN_PRIVKEY/

Title: Quantum DXi V1000 SSH Private Key Exposure

Type: metasploit

Description: Quantum ships a public/private key pair on DXi V1000 2.2.1 appliances that allows passwordless authentication to any other DXi box. Since the key is easily retrievable, an attacker can use it to gain unauthorized remote access as root.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/MICROFOCUS_OBR_SHRBOADMIN/

Title: Micro Focus Operations Bridge Reporter shrboadmin default password

Type: metasploit

Description: This module abuses a known default password on Micro Focus Operations Bridge Reporter. The 'shrboadmin' user, installed by default by the product has the password of 'shrboadmin', and allows an attacker to login to the server via SSH. This module has been tested with Micro Focus Operations Bridge Manager 10.40. Earlier versions are most likely affected too. Note that this is only exploitable in Linux installations.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/MERCURIAL_SSH_EXEC/

Title: Mercurial Custom hg-ssh Wrapper Remote Code Exec

Type: metasploit

Description: This module takes advantage of custom hg-ssh wrapper implementations that don't adequately validate parameters passed to the hg binary, allowing users to trigger a Python Debugger session, which allows arbitrary Python code execution.

Score: 0.0

Exploit cvss id:

MSF:EXPLOIT/LINUX/SSH/LOADBALANCERORG_ENTERPRISE_KNOWN_PRIVKEY/

Title: Loadbalancer.org Enterprise VA SSH Private Key Exposure

Type: metasploit

Description: Loadbalancer.org ships a public/private key pair on Enterprise virtual appliances version 7.5.2 that allows passwordless authentication to any other LB Enterprise box. Since the key is easily retrievable, an attacker can use it to gain unauthorized remote access as root.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/IBM_DRM_A3USER/

Title: IBM Data Risk Manager a3user Default Password

Type: metasploit

Description: This module abuses a known default password in IBM Data Risk Manager. The 'a3user' has the default password 'idrm' and allows an attacker to log in to the virtual appliance via SSH. This can be escalate to full root access, as 'a3user' has sudo access with the default password. At the time of disclosure this was an Oday, but it was later confirmed and patched by IBM. Versions <= 2.0.6.1 are confirmed to be vulnerable.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/F5_BIGIP_KNOWN_PRIVKEY/

Title: F5 BIG-IP SSH Private Key Exposure

Type: metasploit

Description: F5 ships a public/private key pair on BIG-IP appliances that allows passwordless authentication to any other BIG-IP box. Since the key is easily retrievable, an

attacker can use it to gain unauthorized remote access as root.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/EXAGRID_KNOWN_PRIVKEY/

Title: ExaGrid Known SSH Key and Default Password

Type: metasploit

Description: ExaGrid ships a public/private key pair on their backup appliances to allow passwordless authentication to other ExaGrid appliances. Since the private key is easily retrievable, an attacker can use it to gain unauthorized remote access as root. Additionally, this module will attempt to use the default password for root, 'inflection'.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/SOLARWINDS_LEM_EXEC/

Title: SolarWinds LEM Default SSH Password Remote Code Execution

Type: metasploit

Description: This module exploits the default credentials of SolarWinds LEM. A menu system is encountered when the SSH service is accessed with the default username and password which is "cmc" and "password". By exploiting a vulnerability that exist on the menuing script, an attacker can escape from restricted shell. This module was tested against SolarWinds LEM v6.3.1.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/VMWARE_VDP_KNOWN_PRIVKEY/

Title: VMware VDP Known SSH Key

Type: metasploit

Description: VMware vSphere Data Protection appliances 5.5.x through 6.1.x contain a known ssh private key for the local user admin who is a sudoer without password.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/UNIX/SSH/ARRAY_VXAG_VAPV_PRIVKEY_PRIVESC/

Title: Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution

Type: metasploit

Description: This module exploits a default hardcoded private SSH key or default hardcoded login and password in the vAPV 8.3.2.17 and vxAG 9.2.0.34 appliances made by Array Networks. After logged in as the unprivileged user, it's possible to modify the world-writable file /ca/bin/monitor.sh with attacker-supplied arbitrary code. Execution is possible by using the backend tool, running setuid, to turn the debug monitoring on. This makes it possible to trigger a payload with root privileges.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/SYMANTEC_SMG_SSH/

Title: Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability

Type: metasploit

Description: This module exploits a default misconfiguration flaw on Symantec Messaging Gateway. The 'support' user has a known default password, which can be used to login to the SSH service, and gain privileged access from remote.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/WINDOWS/SSH/SYSAX_SSH_USERNAME/

Title: Sysax 5.53 SSH Username Buffer Overflow

Type: metasploit

Description: This module exploits a vulnerability found in Sysax's SSH service. By supplying a long username, the SSH server will copy that data on the stack without proper bounds

checking, therefore allowing remote code execution under the context of the user. Please note that previous versions (before 5.53) are also affected by this bug.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/CISCO_UCS_SCPUSER/

Title: Cisco UCS Director default scpuser password

Type: metasploit

Description: This module abuses a known default password on Cisco UCS Director. The 'scpuser' has the password of 'scpuser', and allows an attacker to login to the virtual appliance via SSH. This module has been tested with Cisco UCS Director virtual machines 6.6.0 and 6.7.0. Note that Cisco also mentions in their advisory that their IMC Supervisor and UCS Director Express are also affected by these vulnerabilities, but this module was not tested with those products.

Score: 0.0

Exploit cvss id: MSF:EXPLOIT/LINUX/SSH/CERAGON_FIBEAIR_KNOWN_PRIVKEY/

Title: Ceragon FibeAir IP-10 SSH Private Key Exposure

Type: metasploit

Description: Ceragon ships a public/private key pair on FibeAir IP-10 devices that allows passwordless authentication to any other IP-10 device. Since the key is easily retrievable, an attacker can use it to gain unauthorized remote access as the "mateidu" user.

Score: 0.0

Exploit cvss id: MSF:AUXILIARY/SCANNER/SSH/LIBSSH_AUTH_BYPASS/

Title: libssh Authentication Bypass Scanner

Type: metasploit

Description: This module exploits an authentication bypass in libssh server code where a USERAUTH_SUCCESS message is sent in place of the expected USERAUTH_REQUEST message. libssh versions 0.6.0 through 0.7.5 and 0.8.0 through 0.8.3 are vulnerable. Note that this module's success depends on whether the server code can trigger the correct (shell/exec) callbacks despite only the state machine's authenticated state being set. Therefore, you may or may not get a shell if the server requires additional code paths to be followed.

Score: 0.0

Exploit cvss id: MSF:AUXILIARY/SCANNER/SSH/JUNIPER_BACKDOOR/

Title: Juniper SSH Backdoor Scanner

Type: metasploit

Description: This module scans for the Juniper SSH backdoor (also valid on Telnet). Any username is required, and the password is <<< %s(un='%s') = %u.

Score: 0.0