

TITLE : UNKNOWN
IP : 162.241.216.11
VERSION : 7.4
DEVICE TYPE : UNKNOWN
OS : UNKNOWN
DOMAINS : [bluehost.com]
HOSTNAMES : [bluehost.com, box5331.bluehost.com]
OPTIONS : {raw='unknown'}
METADATA : {crawler='3236b3c035ee7c860908ea10b5fd5a14d78bbb13', id='a7f582ab-9f6c-4fbc-b6c5-a5b56e278f2a', module='ftp'}
PORT : 21
DATA : 220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 150 allowed.
220-Local time is now 08:06. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
421 Can't change directory to /var/ftp/ [/]
211-Extensions supported:
UTF8
EPRT
IDLE
MDTM
SIZE
MFMT
REST STREAM
MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*;
MLSD
PRET
AUTH TLS
PBSZ
PROT
TVFS
ESTA
PASV
EPSV
SPSV
ESTP
211 End.

LOCATION : {areaCode=0, latitude=40.23384, longitude=-111.65853, city='Provo',
regionCode='UT', postalCode='unknown', dmaCode='unknown', countryCode='US',
countryCode3='unknown', countryName='United States'}

SSL INFO : com.fooock.shodan.model.banner.SslInfo@578f2383

=====

ORGANIZATION : Unified Layer

Vulnerabilities : [CVE-2018-20685, CVE-2017-15906, CVE-2021-36368, CVE-2020-14145,
CVE-2018-15473, CVE-2020-15778, CVE-2021-41617, CVE-2018-15919, CVE-2016-20012,
CVE-2019-6110, CVE-2019-6111, CVE-2019-6109]

===== CVE-2021-36368 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character
encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can
employ crafted object names to manipulate the client output, e.g., by using ANSI control
codes to hide additional files being transferred. This affects refresh_progress_meter() in
progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH

===== CVE-2020-14145 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character
encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can
employ crafted object names to manipulate the client output, e.g., by using ANSI control
codes to hide additional files being transferred. This affects refresh_progress_meter() in

progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH

===== CVE-2018-20685 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH

===== CVE-2021-41617 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in

progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH

===== CVE-2018-15473 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH

===== CVE-2020-15778 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in

progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH

===== CVE-2017-15906 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH

===== CVE-2019-6111 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in

progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH

===== CVE-2018-15919 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH

===== CVE-2019-6110 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in

progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH

===== CVE-2019-6109 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH

===== CVE-2016-20012 =====

AVAILABILITYIMPACT : NONE

DESCRIPTION : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in

progressmeter.c.

PUBLISHED : 2019-01-31T18:29:00.710

PRIVILEGESREQUIRED : NONE

VERSION : 3.1

USERINTERACTION : REQUIRED

BASESEVERITY : MEDIUM

CONFIDENTIALITYIMPACT : HIGH

CVE_ID : CVE-2019-6109

ATTACKCOMPLEXITY : HIGH

SCOPE : UNCHANGED

ATTACKVECTOR : NETWORK

INTEGRITYIMPACT : HIGH