UBUNTU_1604_NO_
Asset Details Report

March 29, 2022 11:50:33 PM UTC
by jsicklick

1. ASSET DETAILS

Host Name

UBUNTU_1604_NO_

IP Address: 192.168.1.26

OS: Ubuntu Linux 16.04

MAC Address: 08:00:27:CA:DE:B0

Asset Discovery Date: February 14, 2022 (43 days ago)

Vulnerabilities Assessed: February 14, 2022 (43 days ago)

2. SUMMARY

105	9	572
Total vulnerabilities	Running Services	Installed Software

3. SOLUTIONS

Risk Score	Fix	Vulnerability Names
3.33k	**Upgrade apache2** Use `apt-get upgrade` to upgrade apache2 to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-26690): Apache HTTP Server vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-44790): Apache HTTP Server vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-44224): Apache HTTP Server vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-40438): Apache HTTP Server regression Ubuntu: (Multiple Advisories) (CVE-2021-34798): Apache HTTP Server regression And 6 more vulnerabilities

2.55k	**Configure SMB signing for Samba**
	Configure Samba to enable or require SMB signing as appropriate. To enable SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:
	`server signing = auto`
	To require SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:
	`server signing = mandatory`
		SMB signing not required
		SMB signing disabled
		SMBv2 signing not required

2.53k	**Upgrade vim** Use `apt-get upgrade` to upgrade vim to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2017-17087): Vim vulnerabilities Ubuntu: USN-5093-1 (CVE-2021-3796): Vim vulnerabilities Ubuntu: USN-5147-1 (CVE-2021-3872): Vim vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2019-20807): Vim vulnerabilities Ubuntu: USN-5147-1 (CVE-2021-3928): Vim vulnerabilities And 4 more vulnerabilities

Risk Score	Fix	Vulnerability Names
1.66k	**Upgrade mysql-server** Use `apt-get upgrade` to upgrade mysql-server to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-2171): MySQL vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-2179): MySQL vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-2389): MySQL vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-2169): MySQL vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-2162): MySQL vulnerabilities And 13 more vulnerabilities
1.3k	**Upgrade intel-microcode** Use `apt-get upgrade` to upgrade intel-microcode to the latest version.	Ubuntu: USN-4985-1 (CVE-2020-24513): Intel Microcode vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2017-5715): Intel Microcode vulnerabilities Ubuntu: USN-4985-1 (CVE-2020-24511): Intel Microcode vulnerabilities Ubuntu: USN-4985-1 (CVE-2020-24489): Intel Microcode vulnerabilities Ubuntu: USN-4985-1 (CVE-2020-24512): Intel Microcode vulnerabilities And 1 more vulnerabilities
1.18k	**Upgrade uidmap** Use `apt-get upgrade` to upgrade uidmap to the latest version.	Ubuntu: USN-5254-1 (CVE-2018-7169): shadow vulnerabilities Ubuntu: USN-5254-1 (CVE-2017-12424): shadow vulnerabilities
1.13k	**Upgrade libcurl3** Use `apt-get upgrade` to upgrade libcurl3 to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-22947): curl regression Ubuntu: (Multiple Advisories) (CVE-2021-22925): curl vulnerability Ubuntu: (Multiple Advisories) (CVE-2021-22946): curl regression Ubuntu: (Multiple Advisories) (CVE-2021-22898): curl vulnerability
947	**Upgrade cron** Use `apt-get upgrade` to upgrade cron to the latest version.	Ubuntu: USN-5259-1 (CVE-2019-9705): Cron vulnerabilities Ubuntu: USN-5259-1 (CVE-2019-9706): Cron vulnerabilities Ubuntu: USN-5259-1 (CVE-2019-9704): Cron vulnerabilities Ubuntu: USN-5259-1 (CVE-2017-9525): Cron vulnerabilities
868	**Upgrade Ubuntu** Upgrade to a supported version of Ubuntu Linux	Obsolete Version of Ubuntu
863	**Upgrade libapache2-mod-php7.0** Use `apt-get upgrade` to upgrade libapache2-mod-php7.0 to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-21705): PHP vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2020-7071): PHP vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2020-7068): PHP vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-21702): PHP vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-21704): PHP vulnerabilities

Risk Score	Fix	Vulnerability Names

753	**Enable GRUB password**
	Set a password in the GRUB configuration file. This is often located in one of several locations, but can really be anywhere:
	`/etc/grub.conf /boot/grub/grub.conf /boot/grub/grub.cfg /boot/grub/menu.lst`
	For all files mentioned above ensure that a password is set or that the files do not exist.
	To set a plain-text password, edit your GRUB configuration file and add the following line before the first uncommented line:
	`password <password>`
	To set an encrypted password, run grub-md5-crypt and use its output when adding the following line before the first uncommented line:
	`password --md5 <encryptedpassword>`
	For either approach, choose an appropriately strong password.
		No password for Grub

752	**Restrict invalid guest logins** In the 'Local Security Settings' feature of the Windows Control Panel, modify the following settings: • Set the 'Local Policies->User Rights Assignment->Deny access to this computer from the network' to include the guest account • Set the 'Local Policies->Security Options->Accounts: Guest account status' to 'Disabled'.	Invalid CIFS Logins Permitted

744	**Disable ICMP redirect support**
	Issue the following commands as root:
	`sysctl -w net.ipv4.conf.all.accept_redirects=0`
	`sysctl -w net.ipv4.conf.default.accept_redirects=0`
	`sysctl -w net.ipv4.conf.all.secure_redirects=0`
	`sysctl -w net.ipv4.conf.default.secure_redirects=0`
	These settings can be added to /etc/sysctl.conf to make them permanent.
		ICMP redirection enabled

739	**Edit '/etc/securetty' entries** Remove all the entries in /etc/securetty except console, tty[0-9]* and vc\[0-9]* Note: ssh does not use /etc/securetty. To disable root login through ssh, use the "PermitRootLogin" setting in /etc/ssh/sshd_config and restart the ssh daemon.	Anonymous root login is allowed

Risk Score	Fix	Vulnerability Names
736	**Reset umask value** To ensure complete access control over newly created files, set the umask value to 077 for root and other user accounts for both interactive and non-interactive processes. The umask value for interactive processes is typically set via PAM. See 'man 8 pam_umask'. For non-interactive processes, /etc/login.defs is a common location for controlling umask on Linux systems. In both cases, you may need to consult your operating system's documentation for the correct file(s) and settings. For Red Hat Enterprise Linux and derivative distributions the umask value is set in /etc/profile and /etc/bashrc shell configuration files. See the Red Hat manual for more details.	User umask value is unsafe
600	**Restrict Query Access on Caching Nameservers** Restrict the processing of DNS queries to only systems that should be allowed to use this nameserver.	DNS server allows cache snooping
584	**Upgrade libgcrypt20** Use `apt-get upgrade` to upgrade libgcrypt20 to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-33560): Libgcrypt vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-40528): Libgcrypt vulnerabilities
583	**Restrict User's home directory mode** Restrict the user home directory mode to at most 750 using the command: `chmod 750 userDir`	User home directory mode unsafe
581	**Partition Mounting Weakness** The specific way to modify the partition mount options varies from system to system. Consult your operating system's manual or mount man page.	Partition Mounting Weakness
579	**Disable HTTP OPTIONS method** Disable HTTP OPTIONS method on your web server. Refer to your web server's instruction manual on how to do this.	HTTP OPTIONS Method Enabled
578	**Disable any MD5 or 96-bit HMAC algorithms within the SSH configuration** Consult the product documentation for instructions to disable any insecure MD5 or 96-bit HMAC algorithms within the SSH configuration.	SSH Weak Message Authentication Code Algorithms
573	**Remove/disable SMB1** For Samba systems on Linux, disabling SMB1 is quite straightforward: How to configure Samba to use SMBv2 and disable SMBv1 on Linux or Unix	SMB: Service supports deprecated SMBv1 protocol
564	**Upgrade liblz4-1** Use `apt-get upgrade` to upgrade liblz4-1 to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-3520): LZ4 vulnerability
563	**Upgrade libx11-6** Use `apt-get upgrade` to upgrade libx11-6 to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-31535): libx11 vulnerability

Risk Score	Fix	Vulnerability Names
474	**Upgrade byobu** Use `apt-get upgrade` to upgrade byobu to the latest version.	Ubuntu: USN-5234-1 (CVE-2019-7306): Byobu vulnerability
436	**Upgrade git** Use `apt-get upgrade` to upgrade git to the latest version.	Ubuntu: USN-5076-1 (CVE-2021-40330): Git vulnerability
345	**Upgrade dbus** Use `apt-get upgrade` to upgrade dbus to the latest version.	Ubuntu: USN-5244-1 (CVE-2020-35512): DBus vulnerability
303	**Upgrade squashfs-tools** Use `apt-get upgrade` to upgrade squashfs-tools to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-40153): Squashfs-Tools vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-41072): Squashfs-Tools vulnerability
295	**Upgrade cpio** Use `apt-get upgrade` to upgrade cpio to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-38185): GNU cpio vulnerability
261	**Upgrade libssl1.0.0** Use `apt-get upgrade` to upgrade libssl1.0.0 to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-3712): EDK II vulnerabilities
244	**Upgrade policykit-1** Use `apt-get upgrade` to upgrade policykit-1 to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-4034): PolicyKit vulnerability
211	**Upgrade libapr1** Use `apt-get upgrade` to upgrade libapr1 to the latest version.	Ubuntu: USN-5056-1 (CVE-2021-35940): APR vulnerability
200	**Restrict Processing of Recursive Queries** Restrict the processing of recursive queries to only systems that should be allowed to use this nameserver.	Nameserver Processes Recursive Queries
188	**Upgrade python3.5** Use `apt-get upgrade` to upgrade python3.5 to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-3733): Python vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-3737): Python vulnerabilities
182	**Upgrade systemd** Use `apt-get upgrade` to upgrade systemd to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2020-13529): systemd vulnerabilities Ubuntu: (Multiple Advisories) (CVE-2021-33910): systemd vulnerabilities
173	**Upgrade ntfs-3g** Use `apt-get upgrade` to upgrade ntfs-3g to the latest version.	Ubuntu: USN-5060-2: NTFS-3G vulnerabilities

Risk Score	Fix	Vulnerability Names
166	**Upgrade ca-certificates** Use `apt-get upgrade` to upgrade ca-certificates to the latest version.	Ubuntu: USN-5089-2: ca-certificates update
155	**Upgrade apport** Use `apt-get upgrade` to upgrade apport to the latest version.	Ubuntu: USN-5122-2: Apport vulnerability
154	**Upgrade ISC BIND to latest version** More information about upgrading your version of ISC BIND is available on the ISC website.	ISC BIND: A query name which is too long can cause a segmentation fault in lwresd (CVE-2016-2775)
148	**Upgrade libglib2.0-data** Use `apt-get upgrade` to upgrade libglib2.0-data to the latest version.	Ubuntu: USN-5189-1 (CVE-2021-3800): GLib vulnerability
144	**Upgrade bind9** Use `apt-get upgrade` to upgrade bind9 to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-25219): Bind vulnerability
105	**Upgrade isc-dhcp-client** Use `apt-get upgrade` to upgrade isc-dhcp-client to the latest version.	Ubuntu: (Multiple Advisories) (CVE-2021-25217): DHCP vulnerability

0	**Disable ICMP timestamp responses on Linux**
	Linux offers neither a sysctl nor a /proc/sys/net/ipv4 interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using iptables, and/or block it at the firewall. For example:
	`ipchains -A input -p icmp --icmp-type timestamp-request -j DROP`
	`ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP`
	The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).
		ICMP timestamp response

0	**Disable TCP timestamp responses on Linux**
	Set the value of net.ipv4.tcp_timestamps to 0 by running the following command:
	`sysctl -w net.ipv4.tcp_timestamps=0`
	Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:
	`net.ipv4.tcp_timestamps=0`
		TCP timestamp response

0	**Restrict access to NetBIOS**	NetBIOS NBSTAT Traffic Amplification
0	**Restrict access to DNS**	DNS Traffic Amplification
0	**Adjust the share permissions to be more secure** Adjust the share permissions to restrict access to only those members of the organization who need the data. It is considered bad practice to grant the "Everyone", "Guest", or "Authenticated Users" groups read or write access to a share.	CIFS Share Readable By Everyone CIFS Share Writeable By Everyone

4. VULNERABILITIES (105)

Vulnerability Name	CVSS Score	Risk Score	Published On	Found	Severity	Solution
Anonymous root login is allowed	6.5	739	Tue, Nov 30, 2004	Tue, Nov 30, 2004	Severe	Solution
CIFS Share Readable By Everyone	0	0.0	Fri, Jan 1, 1999	Thu, Jan 19, 2017	Moderate	Solution
CIFS Share Writeable By Everyone	0	0.0	Fri, Jan 1, 1999	Thu, Jan 19, 2017	Moderate	Solution
DNS server allows cache snooping	5	600	Mon, Jan 1, 1990	Fri, Apr 1, 2011	Severe	Solution
DNS Traffic Amplification	0	0.0	Fri, Mar 29, 2013	Wed, Dec 10, 2014	Moderate	Solution
HTTP OPTIONS Method Enabled	2.6	579	Fri, Oct 7, 2005	Tue, Aug 28, 2018	Moderate	Solution
ICMP redirection enabled	6.8	744	Wed, Dec 31, 2003	Tue, Nov 30, 2004	Severe	Solution
ICMP timestamp response	0	0.0	Fri, Aug 1, 1997	Mon, Nov 1, 2004	Moderate	Solution
Invalid CIFS Logins Permitted	7.5	752	Tue, Jan 25, 2005	Tue, Jan 25, 2005	Critical	Solution
ISC BIND: A query name which is too long can cause a segmentation fault in lwresd (CVE-2016-2775)	5.9	154	Tue, Jul 19, 2016	Tue, Aug 2, 2016	Severe	Solution
Nameserver Processes Recursive Queries	5	200	Mon, Jan 1, 1990	Fri, Feb 26, 2010	Severe	Solution
NetBIOS NBSTAT Traffic Amplification	0	0.0	Sun, Feb 9, 2014	Wed, Dec 10, 2014	Moderate	Solution
No password for Grub	4.6	753	Fri, Jan 1, 1999	Tue, Nov 30, 2004	Severe	Solution
Obsolete Version of Ubuntu	10	868	Mon, May 6, 2013	Mon, May 6, 2013	Critical	Solution
Partition Mounting Weakness	1.9	581	Sat, Jan 15, 2005	Sat, Jan 15, 2005	Moderate	Solution
SMB signing disabled	7.3	851	Mon, Nov 1, 2004	Fri, Apr 1, 2011	Severe	Solution
SMB signing not required	6.2	848	Mon, Nov 1, 2004	Fri, Apr 1, 2011	Severe	Solution
SMB: Service supports deprecated SMBv1 protocol	4.8	573	Tue, Apr 21, 2015	Thu, Apr 11, 2019	Severe	Solution
SMBv2 signing not required	6.2	848	Mon, Nov 1, 2004	Wed, Feb 21, 2018	Severe	Solution
SSH Weak Message Authentication Code Algorithms	4	578	Mon, Jan 6, 2014	Tue, Mar 31, 2020	Severe	Solution
TCP timestamp response	0	0.0	Fri, Aug 1, 1997	Fri, Apr 1, 2011	Moderate	Solution
Ubuntu: (Multiple Advisories) (CVE-2017-17087): Vim vulnerabilities	5.5	398	Fri, Dec 1, 2017	Thu, Oct 15, 2020	Moderate	Solution
Ubuntu: (Multiple Advisories) (CVE-2017-5715): Intel Microcode vulnerabilities	5.6	371	Thu, Jan 4, 2018	Sat, Jan 6, 2018	Moderate	Solution
Ubuntu: (Multiple Advisories) (CVE-2019-20807): Vim vulnerabilities	5.3	347	Thu, May 28, 2020	Thu, Oct 15, 2020	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2020-13529): systemd vulnerabilities	6.1	70.0	Mon, May 10, 2021	Wed, Jul 21, 2021	Moderate	Solution

Vulnerability Name	CVSS Score	Risk Score	Published On	Found	Severity	Solution
Ubuntu: (Multiple Advisories) (CVE-2020-35452): Apache HTTP Server vulnerabilities	7.3	309	Thu, Jun 10, 2021	Mon, Jun 21, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2020-7068): PHP vulnerabilities	3.6	259	Mon, Jul 6, 2020	Thu, Jul 8, 2021	Moderate	Solution
Ubuntu: (Multiple Advisories) (CVE-2020-7071): PHP vulnerabilities	5.3	189	Thu, Jan 14, 2021	Thu, Jul 8, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2146): MySQL vulnerabilities	4.9	67.0	Thu, Apr 22, 2021	Thu, May 13, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2154): MySQL vulnerabilities	4.9	67.0	Thu, Apr 22, 2021	Thu, May 13, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2162): MySQL vulnerabilities	4.3	84.0	Thu, Apr 22, 2021	Thu, May 13, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2166): MySQL vulnerabilities	4.9	67.0	Thu, Apr 22, 2021	Thu, May 13, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2169): MySQL vulnerabilities	4.9	67.0	Thu, Apr 22, 2021	Thu, May 13, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-21702): PHP vulnerabilities	7.5	151	Mon, Feb 15, 2021	Thu, Jul 8, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-21704): PHP vulnerabilities	5.9	80.0	Wed, Jul 7, 2021	Thu, Jul 8, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-21705): PHP vulnerabilities	5.3	184	Wed, Jul 7, 2021	Thu, Jul 8, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2171): MySQL vulnerabilities	4.4	54.0	Thu, Apr 22, 2021	Thu, May 13, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2179): MySQL vulnerabilities	4.9	67.0	Thu, Apr 22, 2021	Thu, May 13, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2180): MySQL vulnerabilities	4.9	67.0	Thu, Apr 22, 2021	Thu, May 13, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2194): MySQL vulnerabilities	4.9	67.0	Thu, Apr 22, 2021	Thu, May 13, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2226): MySQL vulnerabilities	4.9	202	Thu, Apr 22, 2021	Thu, May 13, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-22898): curl vulnerability	3.1	165	Wed, May 26, 2021	Fri, Jul 23, 2021	Moderate	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-22925): curl vulnerability	5.3	439	Wed, Jul 21, 2021	Fri, Jul 23, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-22946): curl regression	7.5	435	Wed, Sep 15, 2021	Thu, Sep 16, 2021	Severe	Solution

Vulnerability Name	CVSS Score	Risk Score	Published On	Found	Severity	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-22947): curl regression	5.9	94.0	Wed, Sep 15, 2021	Thu, Sep 16, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2307): MySQL vulnerabilities	6.1	195	Thu, Apr 22, 2021	Thu, May 13, 2021	Moderate	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2342): MySQL vulnerabilities	4.9	61.0	Wed, Jul 21, 2021	Tue, Jul 27, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2372): MySQL vulnerabilities	4.4	47.0	Wed, Jul 21, 2021	Tue, Jul 27, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2385): MySQL vulnerabilities	5	94.0	Wed, Jul 21, 2021	Tue, Jul 27, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2389): MySQL vulnerabilities	5.9	138	Wed, Jul 21, 2021	Tue, Jul 27, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-2390): MySQL vulnerabilities	5.9	138	Wed, Jul 21, 2021	Tue, Jul 27, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-25217): DHCP vulnerability	7.4	105	Wed, May 26, 2021	Fri, May 28, 2021	Moderate	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-25219): Bind vulnerability	5.3	144	Wed, Oct 27, 2021	Fri, Oct 29, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-26690): Apache HTTP Server vulnerabilities	7.5	148	Thu, Jun 10, 2021	Mon, Jun 21, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-26691): Apache HTTP Server vulnerabilities	9.8	561	Thu, Jun 10, 2021	Mon, Jun 21, 2021	Critical	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-30641): Apache HTTP Server vulnerabilities	5.3	184	Thu, Jun 10, 2021	Mon, Jun 21, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-31535): libx11 vulnerability	9.8	563	Tue, May 25, 2021	Wed, May 26, 2021	Critical	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-33193): Apache HTTP Server regression	7.5	182	Mon, Aug 16, 2021	Tue, Sep 28, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-33560): Libgcrypt vulnerabilities	7.5	443	Tue, Jun 8, 2021	Fri, Sep 17, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-33910): systemd vulnerabilities	5.5	113	Tue, Jul 20, 2021	Wed, Jul 21, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-34798): Apache HTTP Server regression	7.5	145	Thu, Sep 16, 2021	Tue, Sep 28, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-3520): LZ4 vulnerability	9.8	564	Fri, May 14, 2021	Thu, May 27, 2021	Critical	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-35604): MariaDB vulnerability	5.5	108	Wed, Oct 20, 2021	Tue, Oct 26, 2021	Severe	Solution

Vulnerability Name	CVSS Score	Risk Score	Published On	Found	Severity	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-35624): MySQL vulnerabilities	4.9	68.0	Wed, Oct 20, 2021	Tue, Oct 26, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-36160): Apache HTTP Server regression	7.5	145	Thu, Sep 16, 2021	Tue, Sep 28, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-3712): EDK II vulnerabilities	7.4	261	Tue, Aug 24, 2021	Wed, Aug 25, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-3733): Python vulnerabilities	6.5	57.0	Thu, Sep 16, 2021	Fri, Sep 17, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-3737): Python vulnerabilities	7.5	131	Thu, Sep 16, 2021	Fri, Sep 17, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-38185): GNU cpio vulnerability	7.8	295	Sun, Aug 8, 2021	Thu, Sep 9, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-39275): Apache HTTP Server regression	9.8	550	Thu, Sep 16, 2021	Tue, Sep 28, 2021	Critical	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-40153): Squashfs-Tools vulnerabilities	8.1	153	Fri, Aug 27, 2021	Tue, Aug 31, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-4034): PolicyKit vulnerability	7.8	244	Tue, Jan 25, 2022	Wed, Jan 26, 2022	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-40438): Apache HTTP Server regression	9	285	Thu, Sep 16, 2021	Tue, Sep 28, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-40528): Libgcrypt vulnerabilities	5.9	141	Mon, Sep 6, 2021	Fri, Sep 17, 2021	Moderate	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-41072): Squashfs-Tools vulnerability	8.1	151	Tue, Sep 14, 2021	Wed, Sep 15, 2021	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-44224): Apache HTTP Server vulnerabilities	8.2	284	Mon, Dec 20, 2021	Fri, Jan 7, 2022	Severe	Solution
Ubuntu: (Multiple Advisories) (CVE-2021-44790): Apache HTTP Server vulnerabilities	9.8	539	Mon, Dec 20, 2021	Fri, Jan 7, 2022	Critical	Solution
Ubuntu: USN-4985-1 (CVE-2020-24489): Intel Microcode vulnerabilities	8.8	256	Wed, Jun 9, 2021	Sat, Jun 12, 2021	Severe	Solution
Ubuntu: USN-4985-1 (CVE-2020-24511): Intel Microcode vulnerabilities	6.5	202	Wed, Jun 9, 2021	Thu, Jun 10, 2021	Moderate	Solution
Ubuntu: USN-4985-1 (CVE-2020-24512): Intel Microcode vulnerabilities	3.3	202	Wed, Jun 9, 2021	Thu, Jun 10, 2021	Moderate	Solution
Ubuntu: USN-4985-1 (CVE-2020-24513): Intel Microcode vulnerabilities	6.5	202	Wed, Jun 9, 2021	Thu, Jun 10, 2021	Moderate	Solution
Ubuntu: USN-4985-1 (CVE-2021-24489): Intel Microcode vulnerabilities	4.8	63.0	Wed, Jun 9, 2021	Thu, Jun 10, 2021	Severe	Solution
Ubuntu: USN-5056-1 (CVE-2021-35940): APR vulnerability	7.1	211	Mon, Aug 23, 2021	Tue, Aug 31, 2021	Severe	Solution

Vulnerability Name	CVSS Score	Risk Score	Published On	Found	Severity	Solution
Ubuntu: USN-5060-2: NTFS-3G vulnerabilities	4.4	173	Tue, Aug 31, 2021	Wed, Sep 1, 2021	Severe	Solution
Ubuntu: USN-5076-1 (CVE-2021-40330): Git vulnerability	7.5	436	Tue, Aug 31, 2021	Tue, Sep 14, 2021	Severe	Solution
Ubuntu: USN-5089-2: ca-certificates update	4.4	166	Thu, Sep 23, 2021	Fri, Sep 24, 2021	Severe	Solution
Ubuntu: USN-5093-1 (CVE-2021-3770): Vim vulnerabilities	7.8	232	Mon, Sep 6, 2021	Wed, Sep 29, 2021	Severe	Solution
Ubuntu: USN-5093-1 (CVE-2021-3778): Vim vulnerabilities	7.8	286	Wed, Sep 15, 2021	Wed, Sep 29, 2021	Severe	Solution
Ubuntu: USN-5093-1 (CVE-2021-3796): Vim vulnerabilities	7.3	286	Wed, Sep 15, 2021	Wed, Sep 29, 2021	Severe	Solution
Ubuntu: USN-5122-2: Apport vulnerability	4.4	155	Tue, Oct 26, 2021	Wed, Oct 27, 2021	Severe	Solution
Ubuntu: USN-5147-1 (CVE-2021-3872): Vim vulnerabilities	7.8	277	Tue, Oct 19, 2021	Tue, Nov 16, 2021	Severe	Solution
Ubuntu: USN-5147-1 (CVE-2021-3903): Vim vulnerabilities	7.8	218	Wed, Oct 27, 2021	Tue, Nov 16, 2021	Severe	Solution
Ubuntu: USN-5147-1 (CVE-2021-3927): Vim vulnerabilities	7.8	273	Fri, Nov 5, 2021	Tue, Nov 16, 2021	Severe	Solution
Ubuntu: USN-5147-1 (CVE-2021-3928): Vim vulnerabilities	7.8	215	Fri, Nov 5, 2021	Tue, Nov 16, 2021	Severe	Solution
Ubuntu: USN-5189-1 (CVE-2021-3800): GLib vulnerability	4.4	148	Tue, Nov 16, 2021	Wed, Dec 15, 2021	Severe	Solution
Ubuntu: USN-5234-1 (CVE-2019-7306): Byobu vulnerability	7.5	474	Fri, Apr 17, 2020	Wed, Jan 19, 2022	Severe	Solution
Ubuntu: USN-5244-1 (CVE-2020-35512): DBus vulnerability	7.8	345	Mon, Feb 15, 2021	Fri, Jan 21, 2022	Severe	Solution
Ubuntu: USN-5254-1 (CVE-2017-12424): shadow vulnerabilities	9.8	665	Fri, Aug 4, 2017	Fri, Jan 28, 2022	Critical	Solution
Ubuntu: USN-5254-1 (CVE-2018-7169): shadow vulnerabilities	5.3	517	Thu, Feb 15, 2018	Fri, Jan 28, 2022	Severe	Solution
Ubuntu: USN-5259-1 (CVE-2017-9525): Cron vulnerabilities	6.7	604	Fri, Jun 9, 2017	Wed, Feb 2, 2022	Severe	Solution
Ubuntu: USN-5259-1 (CVE-2019-9704): Cron vulnerabilities	5.5	114	Mon, Mar 11, 2019	Wed, Feb 2, 2022	Moderate	Solution
Ubuntu: USN-5259-1 (CVE-2019-9705): Cron vulnerabilities	5.5	114	Mon, Mar 11, 2019	Wed, Feb 2, 2022	Moderate	Solution
Ubuntu: USN-5259-1 (CVE-2019-9706): Cron vulnerabilities	5.5	114	Mon, Mar 11, 2019	Wed, Feb 2, 2022	Moderate	Solution
User home directory mode unsafe	2.1	583	Sat, Jan 15, 2005	Sat, Jan 15, 2005	Moderate	Solution
User umask value is unsafe	4.4	736	Sat, Jan 15, 2005	Sat, Jan 15, 2005	Severe	Solution