

SECURITY	ISSUE	STATUS	DATE	DESCRIPTION	RESOLUTION	STATUS
SECURITY-2020-0001	Buffer overflow in the kernel	Fixed	2020-01-01	A buffer overflow vulnerability in the kernel was identified, allowing a local user to execute arbitrary code with root privileges.	Updated to version 4.19.0-12-amd64	Resolved
SECURITY-2020-0002	Denial of service in the network stack	Fixed	2020-01-05	A denial of service vulnerability in the network stack was identified, allowing an attacker to crash the system by sending a specially crafted packet.	Updated to version 4.19.0-13-amd64	Resolved
SECURITY-2020-0003	Information disclosure in the file system	Fixed	2020-01-10	An information disclosure vulnerability in the file system was identified, allowing an attacker to read sensitive information from the system's memory.	Updated to version 4.19.0-14-amd64	Resolved
SECURITY-2020-0004	Privilege escalation in the shell	Fixed	2020-01-15	A privilege escalation vulnerability in the shell was identified, allowing a local user to gain root access without a password.	Updated to version 4.19.0-15-amd64	Resolved
SECURITY-2020-0005	Remote code execution in the web server	Fixed	2020-01-20	A remote code execution vulnerability in the web server was identified, allowing an attacker to execute arbitrary code on the server.	Updated to version 4.19.0-16-amd64	Resolved
SECURITY-2020-0006	Denial of service in the database engine	Fixed	2020-01-25	A denial of service vulnerability in the database engine was identified, allowing an attacker to crash the database server.	Updated to version 4.19.0-17-amd64	Resolved
SECURITY-2020-0007	Information disclosure in the mail server	Fixed	2020-01-30	An information disclosure vulnerability in the mail server was identified, allowing an attacker to read sensitive information from the server's memory.	Updated to version 4.19.0-18-amd64	Resolved
SECURITY-2020-0008	Privilege escalation in the system services	Fixed	2020-02-05	A privilege escalation vulnerability in the system services was identified, allowing a local user to gain root access.	Updated to version 4.19.0-19-amd64	Resolved
SECURITY-2020-0009	Remote code execution in the API	Fixed	2020-02-10	A remote code execution vulnerability in the API was identified, allowing an attacker to execute arbitrary code on the server.	Updated to version 4.19.0-20-amd64	Resolved
SECURITY-2020-0010	Denial of service in the search engine	Fixed	2020-02-15	A denial of service vulnerability in the search engine was identified, allowing an attacker to crash the search engine.	Updated to version 4.19.0-21-amd64	Resolved
SECURITY-2020-0011	Information disclosure in the logging system	Fixed	2020-02-20	An information disclosure vulnerability in the logging system was identified, allowing an attacker to read sensitive information from the system's logs.	Updated to version 4.19.0-22-amd64	Resolved
SECURITY-2020-0012	Privilege escalation in the system utilities	Fixed	2020-02-25	A privilege escalation vulnerability in the system utilities was identified, allowing a local user to gain root access.	Updated to version 4.19.0-23-amd64	Resolved
SECURITY-2020-0013	Remote code execution in the web framework	Fixed	2020-03-01	A remote code execution vulnerability in the web framework was identified, allowing an attacker to execute arbitrary code on the server.	Updated to version 4.19.0-24-amd64	Resolved
SECURITY-2020-0014	Denial of service in the network protocols	Fixed	2020-03-05	A denial of service vulnerability in the network protocols was identified, allowing an attacker to crash the system by sending a specially crafted packet.	Updated to version 4.19.0-25-amd64	Resolved
SECURITY-2020-0015	Information disclosure in the system logs	Fixed	2020-03-10	An information disclosure vulnerability in the system logs was identified, allowing an attacker to read sensitive information from the system's logs.	Updated to version 4.19.0-26-amd64	Resolved
SECURITY-2020-0016	Privilege escalation in the system services	Fixed	2020-03-15	A privilege escalation vulnerability in the system services was identified, allowing a local user to gain root access.	Updated to version 4.19.0-27-amd64	Resolved
SECURITY-2020-0017	Remote code execution in the API	Fixed	2020-03-20	A remote code execution vulnerability in the API was identified, allowing an attacker to execute arbitrary code on the server.	Updated to version 4.19.0-28-amd64	Resolved
SECURITY-2020-0018	Denial of service in the database engine	Fixed	2020-03-25	A denial of service vulnerability in the database engine was identified, allowing an attacker to crash the database server.	Updated to version 4.19.0-29-amd64	Resolved
SECURITY-2020-0019	Information disclosure in the mail server	Fixed	2020-03-30	An information disclosure vulnerability in the mail server was identified, allowing an attacker to read sensitive information from the server's memory.	Updated to version 4.19.0-30-amd64	Resolved
SECURITY-2020-0020	Privilege escalation in the system utilities	Fixed	2020-04-05	A privilege escalation vulnerability in the system utilities was identified, allowing a local user to gain root access.	Updated to version 4.19.0-31-amd64	Resolved