Search

Home Files News About Contact &[SERVICES_TAB] Add New

Microsoft OMI Management Interface Authentication Bypass

Authored by Spencer McIntyre, Nir Ohfeld, Shir Tamari | Site metasploit.com

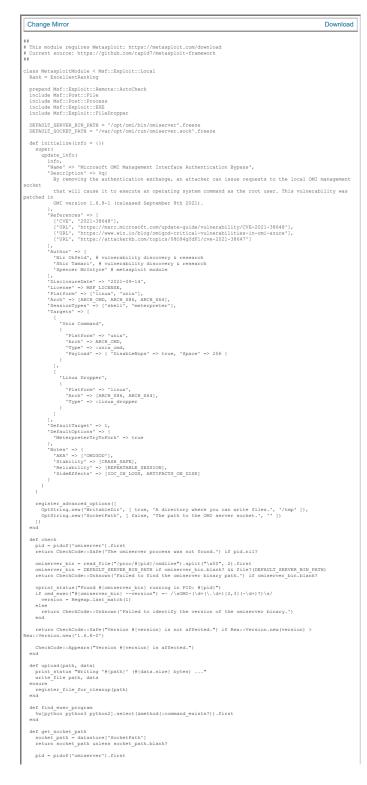
Posted Nov 10, 2021

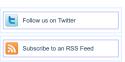
This Metasploit module demonstrates that by removing the authentication exchange, an attacker can issue requests to the local OMI management socket that will cause it to execute an operating system command as the root user. This vulnerability was patched in OMI version 1.6.8-1 (released September 8th 2021).

advisories | CVE-2021-38648

Share This

LinkedIn Reddit Digg StumbleUpon Like TWAS







Top Authors In Last 30 Days Red Hat 157 files Ubuntu 76 files LiquidWorm 23 files Debian 21 files nu11secur1ty 11 files Gentoo 9 files Google Security Research 8 files Julien Ahrens 4 files T. Weber 4 files

Elle Aughborn

Elle Terre

File Tags	File Archives
ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (6,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	
File Upload (946)	Systems
Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

Login or Register to add favorites

packet storm

Site Links A

News by Month News Tags

Files by Month

riles by Monti

File Tags

File Directory

About Us

History & Purpose

Contact Information
Terms of Service

Privacy Statement

Copyright Information

Hosting By

Rokasec





SUSE (1,444)

UNIX (9,159)

Windows (6,511)

Other

SQL Injection (16,102) Ubuntu (8,199)

Spoof (2,166)

TCP (2,379)

Trojan (686) UDP (876)

Virus (662)

Web (9,365) Whitepaper (3,729)

x86 (946) XSS (17,494)

Other

Vulnerability (31,136)