





 **MSRC** | Security Updates  Acknowledgements

   Sign in 



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking “Manage Cookies” at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

AcceptRejectManage cookies

[MSRC](#) > [Customer Guidance](#) > [Security Update Guide](#) > [Advisories](#) > **[CVE 2019 1388](#)**


# Windows Certificate Dialog Elevation of Privilege Vulnerability


CVE-2019-1388


Security Vulnerability


Released: Nov 12, 2019


Assigning CNA: Microsoft


[CVE-2019-1388](#) 

On this page 

 [Subscribe](#)

 [RSS](#)

 [PowerShell](#)

 [API](#)

## Executive Summary

An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data.

To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.

The security update addresses the vulnerability by ensuring Windows Certificate Dialog properly enforces user privileges.

## Exploitability

The following table provides an [exploitability assessment](#) for this vulnerability at the time of original publication.

Publicly disclosed	No
Exploited	No
Exploitability assessment	Exploitation Less Likely

## Acknowledgements

Eduardo Braun Prado working with [Trend Micro's Zero Day Initiative](#)


Microsoft recognizes the efforts of those in the security community who help us protect customers through coordinated vulnerability disclosure. See [Acknowledgements](#) for more information.


## Security Updates


To determine the support lifecycle for your software, see the [Microsoft Support Lifecycle](#).


Updates

CVSS

 Edit columns

 Download

 Filters

Release d... 	Product	Platform	Impact	Max Severity	Article	Dc

Page 1 of 1