Project Zero

Search Project Zero Issues

Sign in

42450276

Commenting

MsMpEng: Remotely Exploitable Type Confusion in Windows 8, 8.1, 10, Windows Server, SCEP, Microsoft Security Essentials, and more.

+1 17   Hotlists   Mark as Duplicate

Comments Dependencies   Duplicates   Blocking   Resources

Fixed   Bug   P2   + Add Hotlist

👥 **STATUS UPDATE** No update yet.

📄 **DESCRIPTION** ta...@google.com created issue #1   May 6, 2017 04:09AM ⋮

[Comment Deleted]

COMMENTS   All comments ▼   ↓ Oldest first

ta...@google.com <ta...@google.com> #2   May 6, 2017 05:38AM ⋮

MSRC Case 38582

ta...@google.com <ta...@google.com> #3   May 7, 2017 12:05AM ⋮

Update from Microsoft.

Hello Tavis,

We have successfully reproduced the issue that you reported to us. We will be finishing our investigation and determining if we will address it in a security release.

Please let me know if you have any additional information that could impact the investigation, or if you have any questions.
----

ta...@google.com <ta...@google.com> #4   May 7, 2017 12:06AM ⋮

Quick second update:

Hi Tavis,

Just wanted to let you know that we are working on fixing this issue. I will continue to provide status updates as they become available.

Thanks again for reporting security issues to Microsoft responsibly and we appreciate your effort in doing so.

----

ta...@google.com <ta...@google.com> #5   May 7, 2017 12:10AM ⋮

[Comment Deleted]

ta...@google.com <ta...@google.com> #6   May 7, 2017 05:23AM ⋮

[Description Changed]

ta...@google.com <ta...@google.com> #7   May 7, 2017 06:16AM ⋮

[Description Changed]

Reporter	👤 ta...@google.com
Type	Bug
Priority	P2
Severity	S0
Status	Fixed
Access	Limited commenting View
Assignee	👤 ta...@google.com
Verifier	--
Collaborators	👥 _____ ⌃
	pr...@google.com
CC	🔔 _____ ⌃
	na...@google.com
	pr...@google.com
	ta...@google.com
Code Changes	--
Pending Code Changes	--
CVE ID	--
Deadline	90 days
Deadline exceeded	No
Finder	natashenka
	taviso
Fixed	--
Grace ext.	No
Methodology	--
Product	Windows
Reported	May 5, 2017
Security Bulletin date	--
Vendor	Microsoft
VendorID	--
Found In	--
Targeted To	--
Verified In	--
In Prod	⬤