CERT-MU Security Alert

CERT-MU

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: 12th July 2017

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Microsoft products and they can be exploited by remote attackers to cause execution of arbitrary code, gain knowledge of sensitive information, take full control of the affected systems and bypass security restrictions. The vulnerabilities reported are as follows:

Vulnerability	Description	Affected Software	Workarounds
Windows Search Object Memory Vulnerability **CVE Info:** CVE-2017-8589	A vulnerability was reported in Windows Search. A remote user can execute arbitrary code on the target system. The vulnerability can be exploited to send specially crafted data via SMB to trigger an object memory handling error and execute arbitrary code on the target system.	Windows 7 SP1 Windows Server 2008 R2 SP1 Windows Server 2008 SP2 Windows Server 2012 Windows 8.1 Windows Server 2012 R2 Windows RT 8.1 Windows 10, Windows Server 2016	Users are advised to apply updates. More information about the updates is available on: https//portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8589
Microsoft HoloLens WiFi Packet Processing Bug **CVE Info:** CVE-2017-8584	A vulnerability has been identified reported in Microsoft HoloLens. This vulnerability can allow a remote attacker to cause execution of arbitrary code on the target system.	Windows 10 Windows Server 2016	Users are advised to apply updates. More information about the updates is available on:

	A remote user on the wireless network can send a specially crafted packet to trigger an object memory handling error and execute arbitrary code on the target system.		https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8584
Microsoft .NET Denial of Service Vulnerability **CVE Info:** CVE-2017-8585	A denial of service vulnerability exists when Microsoft Common Object Runtime Library improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET web application. This vulnerability can be exploited by issuing specially crafted requests to the .NET application.	Microsoft .NET versions 4.6, 4.6.1, 4.6.2, 4.7	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8585
Https.sys Information Disclosure Vulnerability **CVE Info:** CVE-2017-8582	A vulnerability has been identified in Windows 'HTTP.sys' Server and can be exploited by remote attackers to obtain potentially sensitive information on the target system. This vulnerability can be exploited by remote attackers to send a specially crafted request to the 'HTTP.sys' server application to trigger an object memory handling error and view potentially sensitive information on the target system.	Windows 7 SP1 Windows Server 2008 R2 SP1 Windows Server 2008 SP2 Windows Server 2012 Windows 8.1 Windows Server 2012 R2 Windows RT 8.1 Windows 10	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8582
Kerberos SNAME Security Feature Bypass Vulnerability **CVE Info:** CVE-2017-8495	A vulnerability has been identified in Windows Kerberos and can be exploited by remote authenticated user to bypass security restrictions. The vulnerability can allow a remote authenticated user to conduct a man-in-the-middle attack and	Windows 7 SP1 Windows Server 2008 R2 SP1 Windows Server 2008 SP2 Windows Server 2012	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-

	modify the SNAME field during ticket exchange to bypass Extended Protection for Authentication controls on the target system	Windows 8.1 Windows Server 2012 R2 Windows RT 8.1 Windows 10	US/security-guidance/advisory/CVE-2017-8495
Microsoft SharePoint Server Input Validation Flaw Lets Remote Authenticated Users Conduct Cross-Site Scripting Attacks **CVE Info:** CVE-2017-8569	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.	SharePoint Enterprise Server 2016	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8569
Microsoft Edge Vulnerabilities **CVE Info:** CVE-2017-8602 CVE-2017-8592	Two vulnerabilities have been reported in Microsoft Edge and they can be exploited by remote to bypass security controls on the target system and spoof content. The vulnerabilities reported are as follows:	Microsoft Edge	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-

	• A remote user can create specially crafted web content that, when loaded by the target user, will bypass CORS restrictions and redirect the target user's browser to restricted URLs. • A remote user can create a specially crafted URL that, when loaded by the target user, will trigger an HTTP content parsing error to redirect the target user to an arbitrary web site and spoof content.		US/security-guidance/advisory/CVE-2017-8592 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8602
Microsoft Internet Explorer Lets Remote Bypass CORS Restrictions and Spoof Content **CVE Info:** CVE-2017-8602 CVE-2017-8592	Two vulnerabilities were reported in Microsoft Internet Explorer. A remote user can bypass security controls on the target system. A remote user can spoof content. A remote user can create specially crafted web content that, when loaded by the target user, will bypass CORS restrictions and redirect the target user's browser to restricted URLs. A remote user can create a specially crafted URL that, when loaded by the target user, will trigger an HTTP content parsing error to redirect the target user to an arbitrary web site and spoof content.	Internet Explorer versions 9, 10, 11	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8592 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8602
Microsoft Edge Lets Remote Bypass Same Origin Policy and	Two vulnerabilities have been identified in Microsoft Edge and they can be exploited by remote attackers	Microsoft Edge	Users are advised to apply updates. More information about

Spoof Content **CVE Info:** CVE-2017-8611 CVE-2017-8599	to bypass security controls and spoof content on the vulnerable system. The vulnerabilities reported are as follows: • A remote user can bypass Same Origin Policy to cause the target user's browser to load a page with arbitrary contents. • A remote user can create a specially crafted URL that, when loaded by the target user, will trigger an HTTP content parsing error to redirect the target user to an arbitrary web site and spoof content.		the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8599 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8611
Microsoft WordPad File Processing Flaw Lets Remote Users Execute Arbitrary Code **CVE Info:** CVE-2017-8588	A vulnerability has been identified in Microsoft WordPad and can be exploited by remote attackers to cause arbitrary code to be executed on the user's system. This vulnerability can allow remote user can create a specially crafted file that, when loaded by the target user, will trigger a parsing error and execute arbitrary code on the target system. The code will run with the privileges of the target user.	Windows 7 SP1 Windows Server 2008 R2 SP1 Windows Server 2008 SP2 Windows Server 2012 Windows 8.1 Windows Server 2012 R2 Windows RT 8.1 Windows 10	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8588

Microsoft Graphics Component Object Memory Handling Errors Let Local Users Gain Elevated Privileges **CVE Info:** CVE-2017-8574 CVE-2017-8573 CVE-2017-8556	Several vulnerabilities were reported in Graphics Component and can allow user to obtain elevated privileges on the target system. The vulnerabilities can allow local user to run a specially crafted application to trigger an object memory handling error and execute arbitrary commands on the target system with kernel-level privileges.	Windows 7 SP1 Windows Server 2008 R2 SP1 Windows Server 2008 SP2 Windows Server 2012 Windows 8.1 Windows Server 2012 R2 Windows RT 8.1 Windows 10	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8573 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8574 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8556
Windows Performance Monitor Console and Windows System Information Console XML External Entity Processing Flaw Lets Remote Users Obtain Potentially Sensitive Information **CVE Info:** CVE-2017-8557 CVE-2017-0170	Two vulnerabilities have been reported in Windows Performance Monitor Console and Windows System Information Console and can allow remote attackers to conduct XML external entity attacks to obtain files on the target system. The vulnerabilities reported are as follows: A remote user can create specially crafted XML External Entity (XXE) file that, when imported by the target user that is a member of the Performance Log Users or Local	Windows 7 SP1 Windows Server 2008 R2 SP1 Windows Server 2008 SP2 Windows Server 2012 Windows 8.1 Windows Server 2012 R2 Windows RT 8.1 Windows 10 Windows Server 2016	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0170

	Administrators group after the target user has created a Data Collector Set, will read arbitrary files on the target system. A remote user can create specially crafted XML External Entity (XXE) file that, when loaded via the Windows System Information Console by the target user, will read arbitrary files on the target system.		
Windows PowerShell Deserialization Error Lets Remote Authenticated Users Execute Arbitrary Code on the Target System **CVE Info:** CVE-2017-8565	A remote code execution vulnerability exists in PowerShell when PSObject wraps a CIM Instance. An attacker who successfully exploited this vulnerability could execute malicious code on a vulnerable system. In an attack scenario, an attacker could execute malicious code in a PowerShell remote session.	Windows 7 SP1 Windows Server 2008 R2 SP1 Windows Server 2008 SP2 Windows Server 2012 Windows 8.1 Windows Server 2012 R2 Windows RT 8.1 Windows 10 Windows Server 2016	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8565

Win32k Elevation of Privilege Vulnerabilities **CVE Info:** CVE-2017-8590 CVE-2017-8581 CVE-2017-8580 CVE-2017-8578 CVE-2017-8577 CVE-2017-8566 CVE-2017-8564 CVE-2017-8486 CVE-2017-8467	Multiple vulnerabilities were reported in Windows Kernel and can allow remote attackers to obtain potentially sensitive information and obtain elevated privileges on the target system. The vulnerabilities reported are as follows: • A local user can run a specially crafted application to trigger a flaw in the Win32 driver and obtain potentially sensitive information on the target system. • A local user can run a specially crafted application to trigger a flaw in the kernel and obtain potentially sensitive information about kernel memory addresses, which may facilitate Kernel Address Space Layout Randomization (KASLR) bypass attacks on the target system. • A local user can run a specially crafted application to trigger an object memory handling error and execute arbitrary commands on the target system with elevated privileges. • The Windows kernel-mode driver is affected. • The Windows Common Log File System (CLFS) driver is affected.	Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1703 for x64-based Systems	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8467 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8486 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8564 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8566 https://portal.msrc.microsoft.com/en-US/security-

	• A local user can run a specially crafted application to trigger a parameter handling flaw in a method of a DCOM class in the Windows Input Method Editor (IME) to gain elevated privileges.		guidance/advisory/CVE-2017-8577 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8578 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8580 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8581 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8590

Microsoft Exchange Input Validation Flaws Let Remote Users Conduct Open Redirect and Cross-Site Scripting Attacks **CVE Info:** CVE-2017-8621 CVE-2017-8560 CVE-2017-8559	Several vulnerabilities were reported in Microsoft Exchange and can be exploited by remote attackers to redirect the target user's browser to an arbitrary site and conduct cross-site scripting attacks. The vulnerabilities reported are as follows: • A remote user can create a URL that, when loaded by the target user, will redirect the target user's browser to an arbitrary site. • The software does not properly filter HTML code from user-supplied input before displaying the input. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the Microsoft Exchange software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.	Microsoft Exchange Server 2010 Service Pack 3 Microsoft Exchange Server 2013 Service Pack 1 Microsoft Exchange Server 2013 Cumulative Update 16 Microsoft Exchange Server 2016 Cumulative Update 5	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8621 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8560 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8559

Windows Explorer Bugs Let Remote Users Deny Service and Execute Arbitrary Code **CVE Info:** CVE-2017-8587 CVE-2017-8463	Two vulnerabilities have been identified in Windows Explorer and they can be exploited by remote attackers to cause arbitrary code to be executed on the target user's system and cause the target system to crash. The vulnerabilities reported are as follows: • A remote user can create a specially crafted HTML containing a reference to a non-existing file that, when loaded by the target user, will cause the target user's system to stop responding. • A remote user can create a specially crafted folder and file on a share that, when loaded by the target user, will trigger a flaw in the handling of executable files and shares during rename operations to execute arbitrary code on the target system. The code will run with the privileges of the target user.	Windows 7 SP1 Windows Server 2008 R2 SP1 Windows Server 2008 SP2 Windows Server 2012 Windows 8.1 Windows Server 2012 R2 Windows RT 8.1 Windows 10 Windows Server 2016	Users are advised to apply updates. More information about the updates is available on: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8587 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8463

Source:

Microsoft Security Bulletins

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8587

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8463

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8565

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8467

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8486

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8564

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8566

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8577

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8578

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8580

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8581

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8590

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0170

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8573

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8574

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8556

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8588

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8599

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8611

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8592

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8602

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8592

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8602

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8569

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8495

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8582

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8585

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8584

http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8589

Security Tracker

http://www.securitytracker.com/id/1038866

http://www.securitytracker.com/id/1038864

http://www.securitytracker.com/id/1038865

http://www.securitytracker.com/id/1038863

http://www.securitytracker.com/id/1038862

http://www.securitytracker.com/id/1038861

http://www.securitytracker.com/id/1038857

http://www.securitytracker.com/id/1038856

http://www.securitytracker.com/id/1038855

http://www.securitytracker.com/id/1038854

http://www.securitytracker.com/id/1038853

http://www.securitytracker.com/id/1038850

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu