siber güvenlik karar destek sistemi

Zafiyet Temelli Tarama Sonuç Raporu

2019-05-15

Tarama Sonucu Bulgular

7

Sistem Temel Risk Skoru

8 / 17

Zafiyet (Tekil / Toplam)

1

Alt Ağ

3

Cihaz

26

Yazılım

13

Port/Servis

Tarama Profili

Tarama Özellikleri

Cihaz-Zafiyet Tarama - Zafiyet Tarama - Hızlı

Tarama Adı

Zafiyet Tarama Hızlı

Başlama Zamanı

2019-03-12 12:51:41+0000

Bitiş Zamanı

2019-03-12 20:43:04+0000

Doğrulama

SMB (Windows)

Tarama Kapsamı

192.168.42.0/24, 192.168.41.0/24, 192.168.43.0/24

Raporlanan Zafiyetler

No	Başlık/Tanım	Cihaz Sayısı	Alt Ağ Sayısı	Konum Sayısı	İş Birimi Sayısı	Temel Risk Skoru	İstismar Edilebilirlik
CVE-2018-8476	Microsoft Windows Dağıtım Hizmetleri TFTP Sunucusu CVE-2018-8476	2	1	1	0	100	Yok
CVE-2018-8544	Microsoft Windows VBScript Motor CVE-2018-8544 Uzaktan Kod Yürütme	2	1	1	0	75	Var
CVE-2018-8553	Microsoft Windows Grafik Bileşeni CVE-2018-8553 Uzaktan Kod Yürütme	2	1	1	0	75	Yok
CVE-2018-8256	Microsoft Windows PowerShell CVE-2018-8256 Uzaktan Kod Yürütme	2	1	1	0	75	Yok
CVE-2018-8450	Microsoft Windows Search CVE-2018-8450'de Uzaktan Kod Yürütme	2	1	1	0	55	Yok
CVE-2018-8552	Microsoft Internet Explorer CVE-2018-8552'de Bellek Bozulması Güvenlik...	2	1	1	0	50	Var
CVE-2018-8570	Microsoft Internet Explorer CVE-2018-8570 Uzaktan Bellek Bozulması Güv...	2	1	1	0	50	Yok
CVE-2018-1851	IBM WebSphere Application Server Liberty CVE-2018-1851 Uzaktan Kod	3	1	1	0	50	Yok

CVE-2018-8476 - Microsoft Windows Dağıtım Hizmetleri TFTP Sunucusu CVE-2018-8476 Uzaktan Kod Yürütme ...

100 (Kritik Risk)	Yok	2	1	1	0
Temel Risk	İstismar Edilebilirlik	Cihaz Sayısı	Alt Ağ Sayısı	Konum Sayısı	İş Birimi Sayısı

Yayınlanma Tarihi : 2018-11-13

Düzenlenme Tarihi : 2019-03-12

Etki Değerleri (CVSS v2)

Önem Derecesi : Yüksek

CVSS Baz Skor : 10.0

CVSS Vektörü : AV:N/AC:L/Au:N/C:C/I:C/A:C

Açıklama

Windows Dağıtım Hizmetleri TFTP Sunucusu'nun bellekteki nesneleri işleme biçiminde bir uzaktan kod yürütme güvenlik açığı bulunmaktadır. Bu, Windows Server 2012 R2, Windows Server 2008, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows Server 2008 R2, Windows 10 Sunucularını etkiler.

İlişkili Ürünler

Cihaz

IP	Temel Risk Skoru	Zafiyet Temel Riski	Tespit Durumu	Tespit Tipi
192.168.41.133	100	100	Tespit edildi	-
192.168.41.188	100	100	Tespit edildi	-

Alt Ağ

Ağ	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
192.168.41.0/24	14	100	2150

Konum

Adı	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
Firewall/IDS/IPS	8	100	2244

İş Birimi

CVE-2018-8544 - Microsoft Windows VBScript Motor CVE-2018-8544 Uzaktan Kod Yürütme Güvenlik Açığı

75 (Yüksek Risk)	Var	2	1	1	0
Temel Risk	İstismar Edilebilirlik	Cihaz Sayısı	Alt Ağ Sayısı	Konum Sayısı	İş Birimi Sayısı

Yayınlanma Tarihi : 2018-11-13
Düzenlenme Tarihi : 2019-03-12

Etki Değerleri (CVSS v2)

Önem Derecesi : Yüksek
CVSS Baz Skor : 9.3
CVSS Vektörü : AV:N/AC:M/Au:N/C:C/I:C/A:C

Açıklama

VBScript motorunun bellekteki nesneleri işleme biçiminde bir uzaktan kod yürütme güvenlik açığı bulunmaktadır; "Windows VBScript Motor Uzaktan Kod Yürütme Güvenlik Açığı". Bu, Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Sunucu 2016, Windows Server 2008 R2, Windows 10, Windows 10 Sunucularını etkiler.

İlişkili Ürünler

Cihaz

IP	Temel Risk Skoru	Zafiyet Temel Riski	Tespit Durumu	Tespit Tipi
192.168.41.133	100	75	Tespit edildi	-
192.168.41.188	100	75	Tespit edildi	-

Alt Ağ

Ağ	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
192.168.41.0/24	14	75	2150

Konum

Adı	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
Firewall/IDS/IPS	8	75	2244

İş Birimi

CVE-2018-8553 - Microsoft Windows Grafik Bileşeni CVE-2018-8553 Uzaktan Kod Yürütme Güvenlik Açığı

75 (Yüksek Risk)	Yok	2	1	1	0
Temel Risk	İstismar Edilebilirlik	Cihaz Sayısı	Alt Ağ Sayısı	Konum Sayısı	İş Birimi Sayısı

Yayınlanma Tarihi : 2018-11-13
Düzenlenme Tarihi : 2019-03-12

Etki Değerleri (CVSS v2)

Önem Derecesi : Yüksek
CVSS Baz Skor : 9.3
CVSS Vektörü : AV:N/AC:M/Au:N/C:C/I:C/A:C

Açıklama

Microsoft Graphics Components'ın bellekteki nesneleri işleme biçiminde bir uzaktan kod yürütme güvenlik açığı bulunmaktadır, yani "Microsoft Graphics Components Uzaktan Kod Yürütme Güvenlik Açığı". Bu, Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Sunucu 2016, Windows Server 2008 R2, Windows 10'u etkiler.

İlişkili Ürünler

Cihaz

IP	Temel Risk Skoru	Zafiyet Temel Riski	Tespit Durumu	Tespit Tipi
192.168.41.188	100	75	Tespit edildi	-
192.168.41.133	100	75	Tespit edildi	-

Alt Ağ

Ağ	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
192.168.41.0/24	14	75	2150

Konum

Adı	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
Firewall/IDS/IPS	8	75	2244

İş Birimi

CVE-2018-8256 - Microsoft Windows PowerShell CVE-2018-8256 Uzaktan Kod Yürütme Güvenlik Açığı

75 (Yüksek Risk)	Yok	2	1	1	0
Temel Risk	İstismar Edilebilirlik	Cihaz Sayısı	Alt Ağ Sayısı	Konum Sayısı	İş Birimi Sayısı

Yayınlanma Tarihi : 2018-11-13
Düzenlenme Tarihi : 2019-03-12

Etki Değerleri (CVSS v2)

Önem Derecesi : Yüksek
CVSS Baz Skor : 9.3
CVSS Vektörü : AV:N/AC:M/Au:N/C:C/I:C/A:C

Açıklama

PowerShell özel hazırlanmış dosyaları düzgün bir şekilde işlemediğinde, "Microsoft PowerShell Uzaktan Kod Yürütme Güvenlik Açığı" gibi bir uzaktan kod yürütme güvenlik açığı bulunmaktadır. Bu, Windows RT 8.1, PowerShell Core 6.0, Microsoft.PowerShell.Archive 1.2.2.0, Windows Server 2016, Windows Server 2012, Windows Server 2008 R2, Windows Server 2019, Windows 7, Windows Server 2012 R2, PowerShell Çekirdek 6.1, Windows 10'u etkiler. Sunucular, Windows 10, Windows 8.1.

İlişkili Ürünler

Cihaz

IP	Temel Risk Skoru	Zafiyet Temel Riski	Tespit Durumu	Tespit Tipi
192.168.41.188	100	75	Tespit edildi	-
192.168.41.133	100	75	Tespit edildi	-

Alt Ağ

Ağ	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
192.168.41.0/24	14	75	2150

Konum

Adı	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
Firewall/IDS/IPS	8	75	2244

İş Birimi

CVE-2018-8450 - Microsoft Windows Search CVE-2018-8450'de Uzaktan Kod Yürütme Güvenlik Açığı

55 (Orta Risk)	Yok	2	1	1	0
Temel Risk	İstismar Edilebilirlik	Cihaz Sayısı	Alt Ağ Sayısı	Konum Sayısı	İş Birimi Sayısı

Yayınlanma Tarihi : 2018-11-13
Düzenlenme Tarihi : 2019-03-12

Etki Değerleri (CVSS v2)

Önem Derecesi : Yüksek
CVSS Baz Skor : 9.0
CVSS Vektörü : AV:N/AC:L/Au:S/C:C/I:C/A:C

Açıklama

Windows Search bellekteki nesneleri işlediğinde, "Windows Search Uzaktan Kod Yürütme Güvenlik Açığı" gibi bir uzaktan kod yürütme güvenlik açığı bulunmaktadır. Bu, Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Sunucu 2016, Windows Server 2008 R2, Windows 10, Windows 10 Sunucularını etkiler.

İlişkili Ürünler

Cihaz

IP	Temel Risk Skoru	Zafiyet Temel Riski	Tespit Durumu	Tespit Tipi
192.168.41.188	100	55	Tespit edildi	-
192.168.41.133	100	55	Tespit edildi	-

Alt Ağ

Ağ	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
192.168.41.0/24	14	55	2150

Konum

Adı	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
Firewall/IDS/IPS	8	55	2244

İş Birimi

CVE-2018-8552 - Microsoft Internet Explorer CVE-2018-8552'de Bellek Bozulması Güvenlik Açığı

50 (Orta Risk)	Var	2	1	1	0
Temel Risk	İstismar Edilebilirlik	Cihaz Sayısı	Alt Ağ Sayısı	Konum Sayısı	İş Birimi Sayısı

Yayınlanma Tarihi : 2018-11-13
Düzenlenme Tarihi : 2019-03-12

Etki Değerleri (CVSS v2)

Önem Derecesi : Yüksek
CVSS Baz Skor : 7.6
CVSS Vektörü : AV:N/AC:H/Au:N/C:C/I:C/A:C

Açıklama

VBScript, hafızasının içeriğini uygunsuz şekilde ifşa ettiğinde bir saldırgana, kullanıcının bilgisayarını veya verilerini daha da tehlikeye atacak bir bilgi sağlayabilecek, örneğin "Windows Komut Dosyası Bozma Motoru Bozulması Güvenlik Açığı" olan bir bilginin açığa çıkması güvenlik açığı bulunmaktadır. Bu, Internet Explorer 9, Internet Explorer 11, Internet Explorer 10'u etkiler.

İlişkili Ürünler

Cihaz

IP	Temel Risk Skoru	Zafiyet Temel Riski	Tespit Durumu	Tespit Tipi
192.168.41.188	100	50	Tespit edildi	-
192.168.41.133	100	50	Tespit edildi	-

Alt Ağ

Ağ	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
192.168.41.0/24	14	50	2150

Konum

Adı	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
Firewall/IDS/IPS	8	50	2244

İş Birimi

CVE-2018-8570 - Microsoft Internet Explorer CVE-2018-8570 Uzaktan Bellek Bozulması Güvenlik Açığı

50 (Orta Risk)	Yok	2	1	1	0
Temel Risk	İstismar Edilebilirlik	Cihaz Sayısı	Alt Ağ Sayısı	Konum Sayısı	İş Birimi Sayısı

Yayınlanma Tarihi : 2018-11-13
Düzenlenme Tarihi : 2019-03-12

Etki Değerleri (CVSS v2)

Önem Derecesi : Yüksek
CVSS Baz Skor : 7.6
CVSS Vektörü : AV:N/AC:H/Au:N/C:C/I:C/A:C

Açıklama

Internet Explorer bellekteki nesnelere yanlış eriştiğinde, "Internet Explorer'da Bellek Bozulması Güvenlik Açığı" gibi bir uzaktan kod yürütme güvenlik açığı bulunmaktadır. Bu, Internet Explorer 11'i etkiler.

İlişkili Ürünler

Cihaz

IP	Temel Risk Skoru	Zafiyet Temel Riski	Tespit Durumu	Tespit Tipi
192.168.41.188	100	50	Tespit edildi	-
192.168.41.133	100	50	Tespit edildi	-

Alt Ağ

Ağ	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
192.168.41.0/24	14	50	2150

Konum

Adı	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
Firewall/IDS/IPS	8	50	2244

İş Birimi

CVE-2018-1851 - IBM WebSphere Application Server Liberty CVE-2018-1851 Uzaktan Kod Yürütme Güvenlik A...

50 (Orta Risk)	Yok	3	1	1	0
Temel Risk	İstismar Edilebilirlik	Cihaz Sayısı	Alt Ağ Sayısı	Konum Sayısı	İş Birimi Sayısı

Yayınlanma Tarihi : 2018-10-31
Düzenlenme Tarihi : 2019-03-12

Etki Değerleri (CVSS v2)

Önem Derecesi : Yüksek
CVSS Baz Skor : 7.5
CVSS Vektörü : AV:N/AC:L/Au:N/C:P/I:P/A:P

Açıklama

IBM WebSphere Application Server Liberty OpenID Connect, uzaktaki bir saldırganın hatalı seri hale getirme nedeniyle sistemde rasgele kod yürütmesine izin verebilir. Saldırganın hizmetine özel hazırlanmış bir istek göndererek, saldırgan rasgele bir kod yürütmek için bu güvenlik açığından yararlanabilir. IBM X-Force Kimliği: 150999.

İlişkili Ürünler

Cihaz

IP	Temel Risk Skoru	Zafiyet Temel Riski	Tespit Durumu	Tespit Tipi
192.168.41.132	50	50	Tespit edildi	-
192.168.41.133	100	50	Tespit edildi	-
192.168.41.188	100	50	Tespit edildi	-

Alt Ağ

Ağ	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
192.168.41.0/24	14	50	2150

Konum

Adı	Temel Risk Skoru	Zafiyet Temel Riski	Toplam Zafiyet
Firewall/IDS/IPS	8	50	2244

İş Birimi

Ek

Uygulanan Filtreler

Portlar :	*Filtre yok.*
Yazılımlar :	*Filtre yok.*
Zafiyetler :	*Filtre yok.*
Cihazlar :	*Filtre yok.*
Alt Ağlar :	*Filtre yok.*
Konumlar :	*Filtre yok.*
İş Birimleri :	*Filtre yok.*
Zafiyet Risk Seviyeleri :	*Kritik Risk, Orta Risk*
Cihaz Risk Seviyeleri :	*Kritik Risk, Orta Risk, Yüksek Risk*