

# **Bir Güvenlik Zaafiyetinin Analizi (Binary Analiz Örneđi)**

**Celil Ünüver , SecurityArchitect**

**celilunuver[n0sp4m]gmail.com**

**www.securityarchitect.org**

## **1-) Güvenlik Bildirisi:**

**Uygulama:** Novell eDirectory 8.8 SP5

**Etkilenen Versiyonlar:** 8.8 SP5 ve önceki sürümler

**Firma:** Novell ( [www.novell.com](http://www.novell.com) )

**Risk Seviyesi:** Orta

**BID:** 36815 ( <http://www.securityfocus.com/bid/36815> )

**Orjinal Bildiri:** <http://www.securityarchitect.org/advisories/securityarchitect-003.txt>

**Yayınlanma Tarihi:** 26 Ekim 2009

**Referans:** Celil Ünüver , SecurityArchitect

## **2-) Güvenlik Zaafiyeti:**

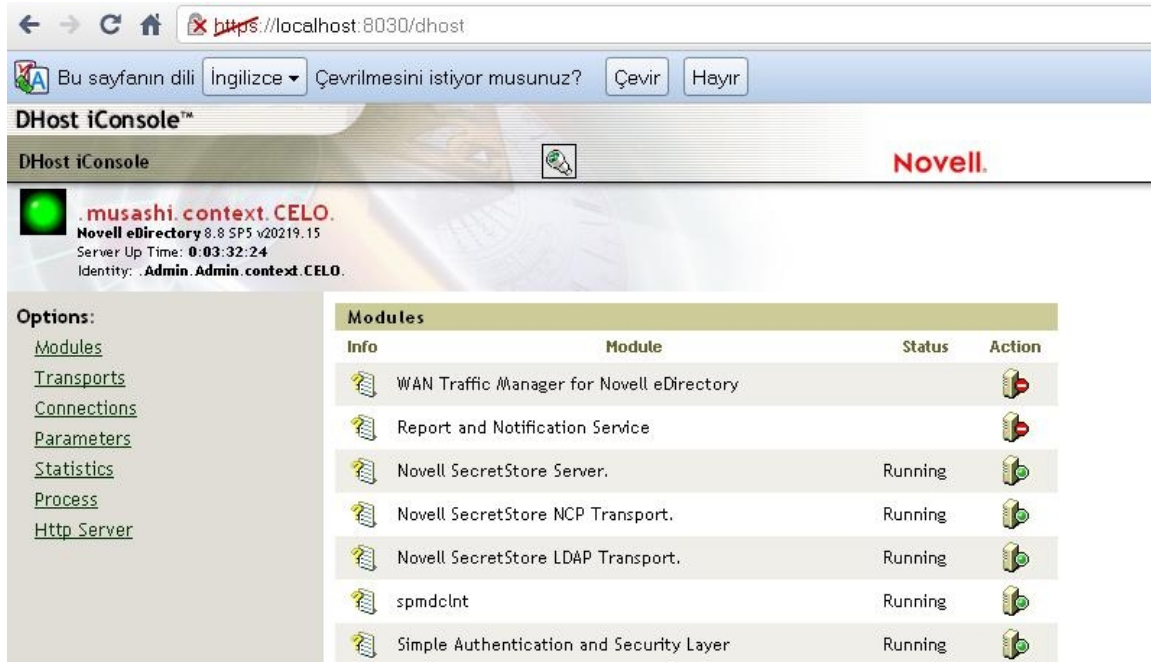
Novell eDirectory' deki bu güvenlik zaafiyeti Dhost süreciyle ilgili bir sorundur. Bu sorun ara bellek taşması (stack buffer overflow) güvenlik zaafiyetine sebebiyet vermektedir. Saldırgan sunucuya kötü niyetli bir istek yollayarak bu zaafiyeti tetikleyebilir ve sonucunda sistemde gelişigüzel (zararlı) kod çalıştırabilir.

## **3-) Yama Durumu:**

Bu açık 26 Ekim 2009 tarihinde 0-day olarak yayınlanmıştır. Firma gerekli yamaları 31 Mayıs 2010 tarihinde yayınlamıştır.

#### 4-) Güvenlik Zaafiyetinin Analizi:

Novell eDirectory Dhost servisi , modül yüklemek , kaldırmak ve modül hakkında bilgi almak için belli adreslere istek yollamaktadır. Sistemdeki mevcut modüllerin ismini kendisi atamaktadır. Aşağıdaki resimde modül listesi ve durumları görülmektedir. Action kısmındaki simgelere tıkladığımızda modülü aktif etmekte ya da aktifse deaktif etmektedir. Örneğin simgesinden de anlaşılacağı gibi Wan Traffic Manager Modülü pasif durumdadır , simgesine tıkladığımızda "<https://localhost:8030/dhost/modules?L:wtm.dlm>" adresine "GET" isteği göndererek modülü aktif etmektedir. Aynı şekilde modules?U: parametresi ile deaktif etmekte ve modules?!: parametresine gönderilen istekle de modül hakkında bilgi vermektedir. Zaafiyet burada modül ismi olarak uzun bir argüman girildiğinde ortaya çıkmaktadır.



The screenshot shows the DHost iConsole web interface. The browser address bar displays <https://localhost:8030/dhost>. The page title is "DHost iConsole™". The interface includes a navigation menu on the left with options like "Modules", "Transports", "Connections", "Parameters", "Statistics", "Process", and "Http Server". The main content area shows a table of modules with columns for "Info", "Module", "Status", and "Action".

Info	Module	Status	Action
	WAN Traffic Manager for Novell eDirectory		
	Report and Notification Service		
	Novell SecretStore Server.	Running	
	Novell SecretStore NCP Transport.	Running	
	Novell SecretStore LDAP Transport.	Running	
	spmdclnt	Running	
	Simple Authentication and Security Layer	Running	

Dhost uygulamasını disassembly edip LoadModule subroutinelerinden birini incelediğimizde zaafiyetin sebebini görmekteyiz ;

```
.text:00408000 ; LMLoadModule(x,x,x,x,x)+C3#  
.text:00408000  
.....  
.....  
.....  
.text:0040802D push offset aS_dlm ; "%s.dlm"  
.text:00408032 lea eax, [ebp+var_24]  
.text:00408035 push eax ; char *  
.text:00408036 call ds:sprintf
```

Görüldüğü gibi Dhost uygulamasında kontrolsüz şekilde sprintf fonksiyonu kullanılmıştır. Fonksiyon modül isminin uzunluğunu kontrol etmiyor , uzun bir modül ismi sisteme gönderildiğinde ara bellek taşması sorununa sebebiyet verecektir.

#### **5-) PoC Exploit:**

<http://www.securityarchitect.org/exploits/novelbof.txt>

#### **6-) Bağlantılar:**

[www.securityarchitect.org](http://www.securityarchitect.org)