

## Customer Problems Discovered, Expedited Remediation using Mu

Mu Dynamics helps network operators and their diverse product suppliers build and operate higher quality, more reliable and robust networks that have minimal downtime. By using the Mu-4000 Analyzer platform, many customers find damaging problems before they occur in production next-gen services, including VoIP, IPTV and IMS-based applications. Here are specific problems discovered and remediated by leading customers at more than 100 deployments including tier one network operators and vendor supplier industries.



### *The Problem Discovered Using Mu*

Operator's FTP application filter dropped sessions erroneously



### *What Could Have Happened if Deployed*

Interruption in legitimate customer traffic, loss of application connectivity



### *How Mu Found the Root Cause*

Mu Service Level Traffic Variations/Protocol Mutation module, FTP option



### *Problem Discovered Using Mu:*

Softswitch SIP traffic was bleeding over to billing system, crippling billing server



### *What Could Have Happened if Deployed:*

Downtime in billing applications cost millions of dollars in lost transaction data and often disrupt customer calls



### *How Mu Found the Root Cause:*

VoIP bundle including SIP in Mu's Service Level Traffic Variations/Protocol Mutation module



### *Problem Discovered Using Mu:*

IPv6 software bug discovered in leading core router vendor, when facing service traffic it caused a broadcast attack



### *What Could Have Happened if Deployed:*

IPv6 weakness would bring down entire cluster of core router, loss of all core and edge IP services depending on router connectivity



### *How Mu Found the Root Cause:*

IPv6 Mu Service Level Traffic Variations/Protocol Mutation module



### *Problem Discovered Using Mu:*

DNS-based DoS VoIP attack weakness in operator network, VoIP domain resolution wiped out with no connectivity



### *What Could Have Happened if Deployed:*

Complete loss of all customer VoIP services for more than 3 hours with hourly cost more than \$150,000 per hour



### *How Mu Found the Root Cause:*

Mu DoS module and DNS using built in and customizable Mu-4000 SIP service monitoring and instrumentation



### *Problem Discovered Using Mu:*

6 month burn in cycle for vendor product roll out at leading network operator costing \$\$\$/time



### *What Could Have Happened if Deployed:*

Limiting service rollout availability



### *How Mu Found the Root Cause:*

Operator and vendor supplier standardize on Mu for service verification and expedited SDLC using SLTV SIP/VoIP



*Problem Discovered Using Mu:*

Incomplete and outdated vulnerability signatures, reliance on exploits instead of underlying vulnerability information caused weakness in deployed network products



*What Could Have Happened if Deployed:*

Malicious exploit of the security products, core network and IP applications.



*How Mu Found the Root Cause:*

Deploying Mu's PVA capabilities to automatically detect and fix a far greater range of published vulnerabilities with fewer IT resources in less time. Significant competitive and time-to-market advantages as well as major cost savings for the vendor's product software development lifecycle (SDLC)



*Problem Discovered Using Mu:*

SSH bug rendered a major Unix-based server platform completely unusable and corrupted the hard drive



*What Could Have Happened if Deployed:*

Had the bug not been found in time, the rollout of a new, vulnerable version of Unix could have cause a major and costly outage of all platform-enabled services



*How Mu Found the Root Cause:*

Methodical and consistent usage of the Mu SLTV module throughout the deployment lifecycle



*Problem Discovered Using Mu:*

DHCP weakness in SOHO firewalls in wide deployment prevents IP connectivity for customers



*What Could Have Happened if Deployed:*

Had this bug been widely exploited or triggered by a worm, large numbers of customers would have lost IP connectivity from their ISP, and the ISP would have had to recall all devices as there was no field remedy



*How Mu Found the Root Cause:*

Methodical and consistent usage of the Mu SLTV module throughout the deployment lifecycle



*Problem Discovered Using Mu:*

Application layer DoS weakness in VoIP softswitch causes loss of service and system crash



*What Could Have Happened if Deployed:*

A SIP DoS attack brought down a core SIP softswitch, and the system was unable to recover without manual intervention. Complete loss of service.



*How Mu Found the Root Cause:*

VoIP bundle including SIP in Mu's Service Level Traffic Variations/Protocol Mutation module



web: [www.mudynamics.com](http://www.mudynamics.com) | email: [info@mudynamics.com](mailto:info@mudynamics.com)  
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA  
phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317